OPEN SOURCE CBDC

EXPLORING OPEN SOURCE IN CBDC DEVELOPMENT: OPPORTUNITIES AND CHALLENGES FOR CENTRAL BANKS

DIGITAL EURO ASSOCIATION
PUBLIC DIGITAL EURO WORKING GROUP

DECEMBER 2024

Open Source CBDC

Exploring Open-source in CBDC Development: Opportunities and Challenges for Central Banks

Chairs

Hubert Knapp

Ritesh Jain

Contributors

Olivier Atangana

Kene Ezeji-Okoye

John Kiff

Conrad Kraft

Brian Mondoh

Karen Ottoni

Lisa-Marie Ross

Frédéric Tronnier

Victor Warhem

The views expressed in this paper are the authors' own and do not necessarily reflect the views of the Digital Euro Association (DEA). The DEA would like to thank its supporting members, whose support was instrumental in making this work possible.

List of Abbreviations

API	Application Programming Interface
B2C	Business-to-Consumer
BISIH	Bank for International Settlements Innovation Hub
CBDC	Central Bank Digital Currency
DLT	Distributed Ledger Technology
ECB	European Central Bank
GPL	General Public License
IBM	International Business Machines Corporation
LEOS	Legislation Editing Open Software
MAS	Monetary Authority of Singapore
MIT	Massachusetts Institute of Technology
NIST	National Institute of Standards and Technology
ONF	Open Networking Foundation
ONOS	Open Network Operating System
OQS	Open Quantum Safe
OSS	Open-Source Software
OSPO	Open Source Program Office
OSI	Open Source Initiative
OSGP	Open Smart Grid Platform
PMC	Project Management Committee
RTPS	Real-Time Payment Systems
rCBDC	Retail Central Bank Digital Currency
RHEL	Red Hat Enterprise Linux
SDN	Software-Defined Networking
SLA	Service Level Agreement
SSRN	Social Science Research Network
UK	United Kingdom
U.S. DoD	United States Department of Defense

Table of Contents

Introduction

Central Bank Digital Currencies (CBDCs) represent a significant evolution in financial infrastructure, offering digital versions of national currencies issued and backed by central banks. They are considered critical financial infrastructure due to their role in the broader economy and the need for zero fault tolerance—any failure could have substantial repercussions. Therefore, ensuring the reliability, security, and adaptability of CBDC systems is paramount. Integrating open-source principles into the development of CBDCs can help achieve these goals, providing transparency, collaboration, and rapid improvements through community contributions.

Open-source solutions could be crucial in building trust and transparency within CBDC projects, especially for retail CBDCs (rCBDC) in regions where consumers and advocacy groups have resisted their implementation. For instance, campaigns like the UK's Big Brother Watch's *NO SPY COIN* initiative highlight public concerns around privacy and surveillance.

By making the source code of CBDC systems publicly accessible, central banks can facilitate independent verification of the software's functionality. This approach could help to address concerns around privacy and surveillance and build confidence among users and stakeholders.

However, building systemically important financial infrastructure, such as a CBDC system, around an open-source core demands meticulous design and evaluation against critical benchmarks, including security, governance, continuity, and expertise. These concerns underscore the need for robust frameworks that balance transparency and collaboration with the operational and regulatory demands of central banks.

Furthermore, embracing an open-source ethos with collaborative input in CBDC design, could also help align the resulting outputs more closely with the public interest, better supporting central banks' public service missions than more opaque, top-down processes.

In light of these considerations, it is prudent that central banks investigate the use of open-source software (OSS) and open licenses when designing and developing CBDCs. This paper aims to explore the role of OSS and its associated methodologies in CBDC development, presenting both its potential benefits and inherent challenges. By analyzing successful case studies and industry best practices, this report seeks to guide central banks in making informed decisions about OSS adoption.

1. The Role of OSS in CBDC Projects

1.1 Introduction to OSS and its Application in CBDCs

OSS development offers a new way to foster an inclusive design process for CBDCs, allowing a broad spectrum of stakeholders to participate rather than confining the design process to a few experts or institutions (Hatunoğlu, 2022). OSS is software whose source code is available for anyone to view, modify, and distribute. The central philosophy of open-source revolves around transparency, community collaboration, and unrestricted access, enabling developers worldwide to contribute to its development and improvement. OSS is typically governed by specific licenses, such as the GNU General Public License (GPL), the MIT License, or the Apache License 2.0, which define how the software can be used and redistributed (covered in more detail below).

Proprietary software is developed, owned, and controlled by a single entity—often a commercial company—that retains exclusive rights over its source code. Users are provided with a license to use the software, but have limited or no access to modify or redistribute it. Proprietary software is restricted to those who purchase or license it, whereas OSS is openly available. Modifications to proprietary software are tightly controlled, whereas anyone can modify and improve OSS. A dedicated in-house team or a commercial for-profit organization or company develops proprietary software, whereas a global community often drives OSS development with a shared mission and, in most cases, a diverse ecosystem of contributors.

The OSS concept shifts power dynamics from a closed, proprietary model—typically governed by service level agreements (SLAs)—to an open, participatory framework. In this framework, diverse stakeholders such as technology providers, potential users, legal experts, academics, government agencies, and civil society organizations collaborate openly through shared access to the software's source code and transparent development practices. This participatory approach, enabled by the principles of OSS, encourages innovation and the development of more robust solutions compared to closed systems. By leveraging OSS methodologies, these diverse groups can contribute to and critique the system in real-time, fostering improvements that lead to a CBDC that is more transparent, inclusive, resilient, adaptable, and publicly accountable. Such transparency and inclusiveness are essential for building public trust and ensuring widespread user acceptance—an achievement that has largely eluded many CBDC projects to date (Kaufmann et al., 2008).

1.2 Case Studies Highlighting OSS in CBDC Development

The 2024 State of Open Source Report underscores the growing importance of OSS in critical infrastructure projects, highlighting its potential for fostering innovation and collaboration across various sectors (OSI, 2024). Key drivers include the desire for cost reduction, transparency, and freedom from vendor lock-in. As CBDCs are increasingly recognized as critical financial infrastructure, open-source principles provide an opportunity to build systems that are transparent, resilient, and aligned with the needs of diverse stakeholders.

One example is OpenCBDC, a joint project between the Massachusetts Institute of Technology (MIT) and the Federal Reserve Bank of Boston (MIT, 2022). Its primary goal is to foster collaborative research on the technical aspects of CBDC design. This project highlights how open source can create neutral platforms where numerous contributors can explore different CBDC architectures, share insights, and contribute to a common technical foundation that benefits the entire ecosystem.

The Bank for International Settlements Innovation Hub' (BISIH) Project Nexus highlights the transformative potential of open-source frameworks in simplifying cross-border payments. By leveraging open Application Programming Interfaces (APIs) and ISO 20022 standards, it enables seamless interoperability between real-time payment systems (RTPS) across jurisdictions. The initiative drives transparency, cost efficiency, and scalability through tools like the Nexus Gateway and its commitment to open-source reference implementations. These efforts create a replicable, adaptable framework that fosters inclusivity and global financial connectivity, offering a practical model for a more efficient and cohesive payment ecosystem (Bank for International Settlements, 2024).

Further demonstrating the potential of OSS in CBDC development is Project Ubin, a pioneering initiative by the Monetary Authority of Singapore (MAS). Conducted between 2016 and 2020, the project explored the use of distributed ledger technology (DLT) for clearing and settling payments and securities. It catalyzed further initiatives to examine potential models for digital currency connectivity. Notably, in 2017, MAS made the source code and technical documentation of three successful DLT-based prototypes publicly available, promoting innovation and collaboration in interbank payments (MAS, 2017). The project underscored several advantages of OSS-based ecosystems, including enhanced transparency and trust, accelerated innovation through diverse contributions, interoperability, cost efficiency, flexibility, and adaptability. However, Project Ubin also highlighted key challenges, such as security risks, lack of control over the project's direction, fragmentation, resource intensity, and regulatory complexities (MAS, 2022).

While pioneering central banks often build their CBDC platforms on OSS components, they have yet to fully embrace open-source development practices in their CBDC initiatives. For instance, the Eastern Caribbean Central Bank's CBDC pilot and Nigeria's launched rCBDCs demonstrate the use of OSS components, such as Hyperledger Fabric, but do not fully adopt open-source development methodologies. This is because their use of open-source components, such as Hyperledger Fabric, is limited to vendor-driven implementations, resulting in centralized control over development rather than fostering a collaborative, community-driven process. Additionally, these projects do not openly share their code or contribute their improvements back to the broader open-source community, which limits transparency and peer review. Such practices fall short of the fundamental principles of open-source development, which emphasize decentralized governance, public access, and shared innovation. In contrast, the Boston Federal Reserve actively participated in MIT's OpenCBDC project, contributing resources and open-sourcing the code on GitHub. Similarly, Norges Bank not only employs open-source technology in its CBDC sandbox experiments but has also published its sandbox for public use and review on GitHub (Norges Bank, 2023).

1.3 Benefits of OSS in CBDC Projects

The case studies discussed above, such as OpenCBDC, Project Ubin, and BISIH Project Nexus, highlight some of the potential benefits offered by OSS and its associated methodologies in CBDC development. The key advantages identified are summarized below, providing an overview of how OSS could contribute to the success of CBDC initiatives.

1.3.1 Transparency and Trust

OSS could enhance transparency by making its source code openly accessible. This openness allows stakeholders to review the code for potential hidden functionalities, such as unauthorized data collection, and verify that the software aligns with privacy and security standards. By fostering greater transparency, OSS may enable central banks to build greater public trust in their CBDC systems, demonstrating a commitment to accountability and security.

1.3.2 User Privacy

Privacy is a critical concern in CBDC systems, given the potential risks of mass surveillance and data misuse. OSS could help address these risks by enabling public scrutiny of the source code, which allows privacy-preserving mechanisms to be identified and verified. Community oversight and independent audits may detect vulnerabilities that could compromise user privacy. This transparency has the potential to reassure the public that their data is protected and that the CBDC system prioritizes privacy by design, at the code-level.

1.3.3 Innovation and Collaboration

OSS methodologies could foster innovation by inviting contributions from a diverse global community of developers, researchers, and stakeholders. These collaborative efforts may enhance the software and create a vibrant ecosystem of ideas and solutions. Such a collaborative environment could allow central banks to access cutting-edge technologies and adapt to evolving needs more effectively.

1.3.4 Interoperability

OSS frameworks often adhere to open standards, such as ISO 20022, which could facilitate seamless integration across payment systems and jurisdictions. Interoperability is particularly important for CBDCs, as it enables them to function effectively in cross-border payment systems and remain compatible with existing financial infrastructure.

1.3.5 Cost Efficiency

By potentially reducing proprietary licensing fees and mitigating vendor lock-in, OSS could offer significant cost savings. Central banks might allocate resources toward system customization and development instead of incurring ongoing expenses for proprietary software. Additionally, shared development costs within the OSS community could further enhance cost efficiency.

1.3.6 Flexibility and Adaptability

OSS could provide the flexibility to tailor systems to specific regulatory, operational, and technological requirements. This adaptability may enable CBDCs to evolve over time, accommodating new functionalities and addressing emerging challenges without being constrained by proprietary limitations.

1.3.7 Public Accountability

The openness inherent in OSS development processes could foster greater public accountability. By making code and development methodologies accessible for scrutiny, central banks could demonstrate a commitment to inclusivity and transparency. This inclusiveness may reinforce trust and align CBDC projects with principles of democratic governance.

1.4 Challenges Associated with OSS in CBDC Systems

While OSS offers numerous benefits, it also introduces distinct challenges that demand careful careful consideration and management. Below is a summary of the key risks associated with the use of OSS in CBDC systems. These potential risks include:

1.4.1 Governance Gaps

With the introduction of OSS, central banks face the risk of misaligned priorities, inefficiencies, and security vulnerabilities without clear governance structures to define roles, responsibilities, baseline security mandates, and other standards. This may involve creating a no-nonsense, results-driven core program steering team (dictators not debaters) responsible for decision-making, while still allowing broader contributions from the community to foster innovation and inclusivity. The intricacies of governance models and their application to OSS in CBDC projects are examined in greater detail in subsequent sections, where strategies for aligning community contributions with institutional objectives are explored.

1.4.2 Security Vulnerabilities

While transparency is a strength of OSS, it also allows malicious actors to identify and exploit potential vulnerabilities. The absence of robust security measures could compromise the integrity of CBDC systems. Regular security audits, code reviews, and penetration testing can help identify and address vulnerabilities proactively. Collaborative scrutiny enables the rapid identification and resolution of vulnerabilities, often more swiftly than in proprietary software environments. This peer review process can contribute to a more resilient and sustainable codebase, as diverse perspectives and expertise help identify, test, and enhance security mechanisms

Initiatives like the Open-source Security Foundation (OpenSSF) enhance security across OSS projects. OpenSSF provides tools and best practices to improve software supply chain security, ensuring that critical dependencies within open-source systems remain secure and well-maintained. By integrating these advanced security frameworks, central banks could more confidently leverage open-source technology without compromising the integrity of the financial systems they oversee.

Further analysis of security frameworks and methodologies for mitigating vulnerabilities in OSS-based CBDC systems is presented later in this paper, offering a comprehensive perspective on maintaining system integrity in mission-critical applications.

1.4.3 Continuity and Vendor Lock-in

While OSS can reduce vendor lock-in, it does not eliminate it fully. Central banks that depend heavily on specific vendors or consultants for customizations and implementations may encounter challenges if those resources become unavailable or unaffordable. To mitigate this risk, central banks could mandate comprehensive knowledge transfer and develop in-house capabilities to effectively manage and maintain their CBDC platforms. By reducing reliance on external vendors and consultants, this approach enhances institutional control, ensures operational continuity, and fosters the long-term sustainability of digital currency initiatives.

1.4.4 Resource and Expertise Challenges

Managing and maintaining OSS may require significant investment in resources and specialized expertise. Central banks, without sufficient in-house capabilities, may become overly reliant on external vendors or the OSS community. This challenge is compounded by the fact that central banks are not typically known for their proficiency in managing large-scale, mission-critical software projects, which require specialized expertise and agile development practices. Developing in-house expertise through training and hiring skilled personnel can reduce dependence on external parties. Establishing knowledge transfer protocols with vendors can also build internal capacity.

1.4.5 Legal and Licensing Risks

The complex nature of OSS licensing introduces potential legal challenges, including misinterpretation or violation of license terms. Incompatibility between different licenses used in OSS components could further complicate CBDC system development and deployment. Conducting thorough legal reviews of OSS licenses and ensuring compatibility between components can help mitigate these risks. Establishing a centralized process for license management can also reduce complexities.

1.4.6 Reputational Risks

System failures, security breaches, or perceived misuse of OSS components in CBDC systems could damage public confidence in both the central bank and the software itself. Transparency, while a strength, could also be misused by critics or malicious actors to undermine trust. Engaging in proactive communication strategies to educate the public on the advantages and safeguards of OSS can build trust. Conducting rigorous testing and validation before deployment can also minimize reputational risks.

2. Licensing and Governance

Adopting OSS and its methodologies presents unique challenges for central banks, particularly in navigating licensing complexities, governance structures, and aligning diverse stakeholders towards a common goal. This section examines how OSS can be fine-tuned to meet the infrastructure demands of CBDCs. It explores key licensing models, governance models, stakeholder roles, and strategies for cultivating a vibrant OSS framework. By addressing these critical intersections of innovation, control, and collaboration, the chapter offers a guide for central banks to more seamlessly integrate OSS into their CBDC initiatives while ensuring security, compliance, and sustainable growth.

2.1 Key Licensing Models

Licenses play a crucial role in the governance of open-source projects, shaping how the software can be used and developed. The most common licenses include:

- **GNU General Public License (GPL)**: This widely used open license allows the freedom to use, modify, and distribute software. Known as a “copyleft” license, derivative works must also be licensed under the GPL to ensure that future generations of the software remain free and open.

- **MIT License**: Known for its minimal restrictions. This license allows anyone to use, modify, distribute, and sublicense the application and source code with minimal restrictions, requiring only the preservation of copyright and license notices.

- **Apache License 2.0**: This license allows anyone to use, modify, and distribute the software, with the additional provision that modified versions must provide a notice of changes. It also includes explicit patent grant provisions for derivative works.

These licenses typically include royalty-free use clauses, meaning the software can be used without paying royalties or licensing fees to the original creator. This encourages broader adoption across industries, as organizations can integrate open-source solutions without incurring additional costs. This has been a significant factor in the growing adoption of OSS, especially for cost-sensitive sectors like government and public services.

2.2 Governance Models

Central banks seeking to leverage OSS for CBDC development must adopt effective governance models to manage how software is contributed, reviewed, and developed. Given the regulatory and operational complexities unique to central banks, careful planning of the project's management is essential. Selecting or adapting an appropriate governance model is critical to ensure alignment with central bank objectives, regulatory standards, and the diverse requirements of CBDC projects.

2.2.1 OSS Approaches

While OSS accelerates innovation by encouraging diverse contributions, it alters the traditional dynamics of the development process. Central banks operate within strict legal and regulatory frameworks that demand rigorous control over their operations.

In contrast, OSS project participants often function outside of these frameworks, presenting central banks with critical decisions on how to engage with OSS technologies and CBDC project participants.

There exists a spectrum of approaches that balance control with innovation:

- **OSS adopter**: In this approach, a central bank leverages open source code bases as a foundation for implementations built internally or with a vendor. The result is more control, which can be critical for regulatory compliance but may limit the innovation and flexibility often associated with open-source projects.

- **OSS collaborator**: The central bank participates in the open source community, sharing requirements and roadmaps, reviewing code, and experimenting with third parties to test interoperability and effectiveness. This approach offers the innovation lift of OSS development but leaves the central bank in control of what features and safeguards it implements.

- **OSS contributor**: Central banks use their expertise and experience to advance the development of a community or projects, contributing developer resources or even code bases. This level of engagement advances the state of innovation for the OSS project and community. Turning software over to the community does decentralize control (to varying degrees depending on the governance models chosen) of the development process for the code base.

2.2.2 OSS Governance Models

Governance models define the roles within the community, including users who leverage the code, contributors who add to it, and maintainers who lead the project by approving or rejecting contributions and determining its strategic direction. Organisations interested in engaging with or initiating an open-source project must carefully consider how the project's development will be managed to align with their goals and priorities. Below are some standard governance models, each suited to different project objectives:

Benevolent Dictatorship

In this model, a single leader—often the project's creator or a core contributor—holds ultimate authority over decisions. While community contributions are encouraged, the leader has the final say, streamlining decision-making and ensuring a unified vision. For an open-source CBDC initiative, a central bank or experienced consortium could assume the "benevolent dictator" role to guide the project's direction while incorporating community input. Examples of this model include the Python and Linux projects, where leaders like Guido van Rossum and Linus Torvalds provided overarching guidance while leveraging contributions from the wider community. Similarly, a lead central bank could maintain consistency and establish a clear roadmap for the CBDC project while drawing on external expertise in certain aspects of development.

Meritocracy

A meritocracy grants influence based on the quality and consistency of contributions. Authority and responsibility are earned through demonstrated value, encouraging innovation and fostering a merit-based path to leadership. For a CBDC project, this model could enable central banks to make significant contributions—such as technological advancements, regulatory frameworks, or code improvements—to gain influence within the project. This approach motivates active participation and collaboration, ensuring that the project benefits from the expertise of committed contributors. The Apache Software Foundation is a notable example of a meritocratic model, where project management committees (PMCs) and committers gain authority through impactful contributions. Similarly, in a meritocratic governance structure for CBDCs, effective contributors, including central banks, would earn a voice in shaping the project while maintaining a collaborative environment.

Open Governance

Open governance prioritises equal participation and community-driven decision-making. In this model, contributors have equal voting rights, ensuring that decisions reflect a broad spectrum of perspectives. For multinational CBDC initiatives, open governance could facilitate balanced decision-making by allowing all participating central banks an equal say, fostering inclusivity and alignment across jurisdictions. The Linux Foundation's Decentralised Trust project exemplifies this approach, enabling community-led development through equal voting rights for contributors. For CBDCs, this model could prevent any single entity, whether a bank or vendor, from dominating the project, fostering an environment where all stakeholders' insights are valued, and trust is built across borders.

Federation

In a federated model, multiple independent teams or entities operate with autonomy under a shared framework. Each sub-group has its own governance process, which allows flexibility while adhering to common standards. For a multinational CBDC project, this would allow each central bank to customize its CBDC implementation to local needs while maintaining interoperability with the larger network. Mozilla exemplifies this model, as various projects and communities operate independently while aligning with Mozilla's overall mission and values. For central banks, a federated approach to a CBDC project could allow each country or region to tailor its CBDC to specific requirements, ensuring local relevance and flexibility without sacrificing international collaboration.

2.2.3 Tiered Governance and Dynamic Adaptation

Building on the governance models discussed above, this section introduces a tiered governance structure tailored to the unique demands of many CBDC projects, emphasizing a balance between open-source collaboration and the regulatory oversight and control required by central banks.

A tiered governance model offers a pragmatic solution to balance public engagement with regulatory oversight in CBDC projects. This approach divides governance responsibilities into technical development, policy-making, and public consultation. For example a public advisory board could ensure community input informs key decisions, while a core technical committee retains ultimate authority over critical system changes.

Beyond role division, a tiered governance model should also address critical concerns such as privacy, transparency, and adaptability. Tools like zero-knowledge proofs or other advanced cryptographic methods allow for public verification of specific governance processes without exposing sensitive information, safeguarding transparency and privacy. Additionally, the governance model should incorporate mechanisms to adapt to technological progress and evolving public expectations. Regular reviews and a transparent, community-driven process for proposing and voting on governance updates can ensure the system remains relevant, secure, and responsive over time.

By carefully designing these governance structures central banks can strike a balance between harnessing the benefits of open-source collaboration and maintaining necessary control and security. Such an approach could address public apprehensions, like those highlighted by the campaigns like the UK's Big Brother Watch's NO SPY COIN, while ensuring compliance with regulatory standards and central bank mandates.

Ultimately, selecting a governance model for an open-source CBDC initiative will hinge on the central bank’s willingness to embrace “openness by design” versus its need for control. As central banks worldwide explore these frameworks, success will lie in achieving the delicate balance between leveraging open source innovation and ensuring the CBDC system remains secure, compliant, and trusted by the public.

2.3 Specific Stakeholder Roles and Responsibilities

The complexity introduced by OSS technologies in CBDC projects stems from the distribution of roles and responsibilities. Below is an outline of how various stakeholders could operate within these governance models:

Central Banks: In any governance model, central banks play the primary role in oversight and regulation. They are responsible for ensuring that the CBDC aligns with their mandates e.g. monetary policy and financial stability. In a federated or decentralized system, this becomes more complex as central banks must also monitor external contributions, ensure compliance across a distributed ecosystem, and manage security risks.

Private Sector: Today, software and consulting companies like Accenture, IBM, or smaller fintech startups play a crucial role in driving innovation, particularly in federated governance models. They collaborate with central banks to introduce new technologies. However, in an OSS model, they also work alongside independent developers and ensure that their contributions meet the rigorous security and regulatory standards set by the central bank.

OSS Community: The OSS community powers much of the transparency in CBDC projects, and this community is made up of participants from central banks, private sector, and others involved in this space. Their contributions—whether in the form of code reviews, feature development, or security patches—are critical to the success of the project. However, managing this community presents governance challenges, especially when it comes to aligning OSS contributions with national or international regulatory requirements.

2.4 Governance Dilemmas

In centralized governance models, integrating open-source contributions often risks stifling the very innovation that OSS is designed to encourage. Centralized control may limit the collaborative and iterative processes that drive open-source innovation, potentially hindering the diversity of ideas and rapid development that characterize OSS projects. Conversely, decentralized models may excel at fostering collaboration but often face difficulties ensuring compliance and maintaining robust security standards. Federated models attempt to strike a middle ground. These models aim to balance central oversight with the flexibility of decentralized contributions but demand highly sophisticated coordination between central authorities and a diverse network of contributors. The success of OSS in CBDC projects lies in navigating this balance—leveraging the strengths of OSS while addressing the inherent governance and compliance challenges it introduces.

3. OSS Security

Security is a cornerstone of CBDC systems, given their role as mission-critical financial infrastructure. This section examines the key security challenges CBDCs face, such as safeguarding transaction integrity, ensuring infrastructure resilience, and protecting data confidentiality. It explores how OSS can contribute to addressing these challenges through established cryptographic standards, rapid vulnerability response, and transparent security practices. Additionally, essential strategies, including fast upgrade cycles, independent security audits, and evolving security measures, to balance the openness of OSS with robust protection against malicious threats, are highlighted.

3.1 Security Challenges in CBDC Systems

Security is the cornerstone of any payment system, and CBDCs, as a new and transformative payment paradigm, demand even higher levels of security. This applies to online transactions and is particularly critical for real time transactions and offline payments (Atangana et al., 2022). Robust security measures are essential to safeguard the integrity of the payment system, ensuring that user funds and the movement of money between participants—users, issuers, and intermediaries—are protected from fraud and external interference.

Effective security in CBDCs requires not only the detection of cyber threats before they arise but also the mitigation of risks from system vulnerabilities. These vulnerabilities may stem from various sources, such as lost or forgotten private keys, flaws in the e-wallet code, or fraud targeting account providers (Kahn & Rivadeneyra, 2020). To address these risks, CBDC systems must adhere to several key security principles (Fanti et al., 2022):

- **Integrity and Balance Conservation**: Ensures that all operations involving minting and fund transfers, such as deposits, redemptions, and settlements, adhere to established monetary policies, thereby guaranteeing the accuracy of the total CBDC supply in circulation.
- **Authorization and Authenticity**: Validates the legitimacy of transactions by verifying user identities and transaction details to prevent unauthorized access or fraudulent activities, where required.
- **Confidentiality**: Safeguards sensitive transaction data through robust encryption techniques, ensuring that privacy is maintained and unauthorized access is prevented.
- **Non-Repudiation**: Ensures that transaction originators cannot deny their actions and that recipients cannot dispute the receipt of payments, thereby providing accountability and transparency.
- **Traceability and Accountability**: Enables comprehensive tracking of transactions to combat money laundering (ML) and the financing of terrorism (CFT), ensuring that all participants in the system are held accountable for their actions, where necessary.
- **Availability and Resilience**: Maintains system reliability and ensures continuous operation even in the face of disruptions, such as server outages or network failures.

Initiatives such as Project Hamilton demonstrate the value of open-source collaboration, enabling rapid detection of code vulnerabilities through community-driven efforts (MIT, 2022). By leveraging open-source frameworks' transparency and collective expertise, CBDCs can achieve robust security that fosters trust and resilience.

3.2 Security of OSS Systems

Security of financial applications and infrastructure are primarily based on cryptography. Best practice development of cryptographic protocols are strongly based on OSS and open-collaboration. This is the so-called Kerckhoffs's principle stating that “a system should be secure even if everything about the system, except the key, is public knowledge” (Shannon, 1949). “Security through obscurity” - meaning code security is based on secret algorithms, is strongly related as an antipattern. Designing a new secure cryptographic algorithm might take years or a decade of world-wide open collaboration. For example, designing the first post-quantum secure cryptographic standard took almost a decade (NIST, 2024).

While cryptography is often regarded as the cornerstone of security in digital systems, non-cryptographic guarantees can also play a significant role in the implementation of digital money systems. These guarantees may include economic mechanisms such as game-theoretical models, institutional safeguards, or multi-institutional (consortium-based) frameworks. Although established best practices for designing the key non-cryptographic components of a CBDC system or financial application are currently lacking, it is widely argued that adopting a principle analogous to Kerckhoff's principle is beneficial. This approach strongly advocates for the use of OSS and open-collaboration frameworks, emphasizing transparency and collective scrutiny to enhance trust and robustness.

Employing OSS for the security features of a system introduces specific challenges. A key concern is that the public nature of OSS may facilitate the rapid detection of security vulnerabilities, including by malicious actors. Consequently, utilizing open-source frameworks for security necessitates meticulous planning and the implementation of additional safeguards, such as:

- **Preparing for Rapid Upgrade Cycles**: To address vulnerabilities promptly, systems should be designed with rapid deployment capabilities for updates, including updates to core cryptographic primitives. This can be achieved through modern practices such as DevOps methodologies, containerized infrastructure, or microservice architectures, with special considerations for cryptographic elements to maintain integrity.
- **Independent Security Audits**: While the open-source model enables community oversight of a system's security, it does not guarantee consistent or systematic feedback. Therefore, regular reviews by independent, professional security auditors are essential to ensure robust security practices and identify vulnerabilities.

- **Adopting Emerging Security Best Practices**: The rapidly evolving landscape of security and privacy necessitates continuous monitoring of the latest advancements, including cryptographic primitives, and their timely integration into the system.

3.3 Quantum Attack Resistance

Designing a payment or CBDC system resilient to quantum adversaries is an urgent challenge. Quantum computers have the ability to solve certain complex mathematical problems significantly faster than classical computers, undermining the cryptographic foundations of current security protocols. This advancement poses a substantial cybersecurity threat for all financial systems.

Developing a future-proof cryptographic framework is complex due to the rapid pace of technological evolution and the time required to implement new cryptographic primitives securely and reliably. Consequently, instead of seeking an unassailable cryptographic solution, it is more practical to adopt a technology management cycle. This approach involves continuously assessing the risks associated with existing cryptographic methods and formulating mitigation strategies to address potential vulnerabilities.

The National Institute of Standards and Technology (NIST) has been actively working on standardizing post-quantum cryptographic algorithms to counteract the threats posed by quantum computing. In August 2024, NIST released the first three finalized post-quantum encryption standards, marking a significant step toward enhancing cryptographic resilience.

The open-source community also plays a crucial role in advancing security research and developing solutions. Projects like the Open Quantum Safe (OQS) initiative aim to support the transition to quantum-resistant cryptography by providing OSS for prototyping quantum-resistant cryptographic algorithms.

Implementing technology management cycles could ensure that cryptographic systems remain adaptable and robust against emerging threats, maintaining the integrity and security of payment and CBDC systems in the quantum era.

4. Cross-Industry Insights

This section highlights how institutions and governments worldwide are employing OSS to drive innovation, enhance transparency, and ensure sustainability across diverse industries. By examining these practices—from banking APIs and smart grid platforms to government-funded digital infrastructure projects—this section identifies strategies and best practices that central banks and financial institutions can adapt to build resilient, collaborative, and future-proof CBDC systems.

4.1 Government Applications of Open-Source in Critical Systems

Institutions worldwide are adopting open-source technology to modernize critical systems, leveraging OSS to drive innovation, reduce dependencies, and enhance resilience in financial infrastructures. This strategic approach fosters digital sovereignty and builds public trust while maintaining essential control over technology stacks. Governments worldwide have increasingly demonstrated the value of open-source strategies in achieving these goals across various sectors, offering valuable lessons for financial services and CBDC development. Notable examples include:

- **German Sovereign Tech Fund:** This initiative supports digital sovereignty by funding the development, improvement, and maintenance of open digital infrastructure, focusing on security, resilience, technological diversity, and the individuals behind the code —a model that could inform CBDC development.

- **U.S. Department of Defense (DoD) Code.mil:** Defense-focused OSS projects like Code.mil emphasize security and collaboration, showcasing strategies that central banks can adapt for secure CBDC frameworks.

- **France's Etalab:** Overseeing data.gouv.fr, Etalab is France's open data and digital transparency initiative, providing public access to government data and resources. It maintains open-source projects on GitHub and encourages contributions from the tech community.

- **European Union's Public Sector:** The EU promotes open-source use through the European Commission Open Source Program Office, managing projects like Joinup, an open-source collaboration platform for public administrations. The EU also contributes to projects such as LEOS (Legislation Editing Open Software), supporting the drafting and sharing of legislative documents.

- **UK Government's Digital Transformation:** The UK developed Gov.UK, a unified digital platform for government services built with OSS and standardized frameworks, enabling seamless integration across departments and agencies. This approach demonstrates how centralized yet open platforms can streamline complex systems—a principle that could be applied to CBDC infrastructure.

4.2 Cross-Industry Open-Source Successes for CBDC Development

The private sector has witnessed numerous successful open-source projects that have shaped and expanded entire ecosystems:

- **Banking Standards:** Open banking mandates that banks share customer data with third-party providers (with consent), developed on open-source standards in the UK and EU. This approach ensures secure, standardized, and regulated access to banking information, fostering a more competitive financial ecosystem.

- **Kubernetes and Red Hat Enterprise Linux (RHEL):** Open-source platforms like Kubernetes, with its dominance in container orchestration, and Red Hat Enterprise Linux, with its enterprise-grade scalability, exemplify how OSS can support large-scale, mission-critical applications—principles that can be applied to CBDC system architectures.

- **Open Smart Grid Platform (OSGP)** is an open-source, vendor-neutral solution advancing smart grid and energy management applications. OSGP streamlines utilities' operations, enabling metering, demand response, and energy storage management across diverse technologies. By 2023, it connected hundreds of thousands of devices to European grids, enhancing interoperability and reducing dependency on proprietary systems. OSGP fosters collaborative innovation, lowers development costs, and minimizes vendor lock-in, driving improved grid efficiency, scalability, and reliability.

5. Conclusion

As central banks explore the potential of CBDCs, incorporating open-source principles offers opportunities to enhance transparency, interoperability, and adaptability. Open-source methodologies, widely proven across industries, provide a collaborative approach that supports innovation and reduces reliance on proprietary systems. For CBDCs, these principles can help establish global standards and foster trust among stakeholders by enabling public and peer review of critical components.

However, open-source adoption is not without challenges. Central banks must address issues such as configuring effective governance models, mitigating security vulnerabilities, ensuring continuity and vendor independence, and investing in the expertise needed for robust implementation. These complexities require careful planning and the integration of best practices, including independent audits, community-driven governance, rapid response mechanisms, and selective open-sourcing of non-critical components to maintain control over sensitive systems.

While not without its complexities, open-source adoption presents a path for developing robust, scalable, and inclusive digital currency systems that are responsive to both current and future needs.

6. Recommendations

Adopt Robust Open-Source Governance

Establish clear governance frameworks to balance collaborative contributions with central bank oversight, ensuring transparency and accountability.

Strengthen Security Measures

Address risks like potential vulnerabilities and continuity challenges by implementing independent audits, adopting best practices, and monitoring emerging security techniques.

Invest in Capacity Building

Develop in-house expertise and training programs to effectively manage and sustain OSS-based CBDC systems.

Promote Transparency and Public Trust

Encourage public and peer review of non-sensitive components to foster trust while maintaining control over critical systems.

Leverage Open Standards for Interoperability

Use open standards and APIs to ensure seamless integration with existing financial systems and cross-border transactions.

Foster Ecosystem Collaboration

Partner with industry stakeholders, academics, and regulators to drive innovation and address implementation challenges through pilots and sandboxes.

References

Atangana, O., Barbier, M., Khoukhi, L., & Royer, W. (2022). Securing Privacy in Offline Payment for Retail Central Bank Digital Currency: A Comprehensive Framework. Proceedings of the 2nd Blockchain and Cryptocurrency Conference (B2C' 2023). https://hal-emse.ccsd.cnrs.fr/GREYC-MONEBIOM/hal-04243732v1

Bank for International Settlements. (2024). Enabling instant cross-border payments: Project Nexus. https://www.bis.org/publ/othp86.pdf

Fanti, G., et al. (2022). Missing key: The challenge of cybersecurity and central bank digital currency. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/

Hatunoğlu, D. C. (2022). A study on understanding the influence of different design approaches to design democratization. Gazi University Journal of Science Part B: Art Humanities Design and Planning, 10(4), 399-413. https://www.researchgate.net/publication/367022336_A_Study_on_Understanding_the_Influence_of_Different_Design_Approaches_to_Design_Democratization

Kahn, C., & Rivadeneyra, F. (2020). Security and convenience of a central bank digital currency. Bank of Canada. https://www.bankofcanada.ca/wp-content/uploads/2020/10/san2020-21.pdf

Kaufmann, D., Kraay, A., & Mastruzzi, M. (2008). Governance matters VII: Aggregate and individual governance indicators 1996-2007. Policy Research Working Paper No. 4654. World Bank, Washington, DC. http://hdl.handle.net/10986/6870

MAS. (2017). Source-codes of successful distributed ledger prototypes publicly released to encourage innovation in inter-bank payments. https://www.mas.gov.sg/news/media-releases/2017/source-codes-of-successful-distributed-ledger-prototypes-publicly-released

MAS. (2022). Ubin+: Advancing cross-border connectivity with wholesale digital currencies. https://www.mas.gov.sg/schemes-and-initiatives/ubin-plus

MIT. (2022). Project Hamilton: Building a hypothetical central bank digital currency. https://dci.mit.edu/project-hamilton-building-a-hypothetical-cbdc

NIST. (2024). NIST releases first 3 finalized post-quantum encryption standards. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Norges Bank. (2023). Smart contracts for the Norges Bank CBDC sandbox. GitHub. https://github.com/norges-bank/cbdc-sandbox-contracts

Open Source Initiative (OSI). (2024). 2024 State of Open Source Report. https://opensource.org/blog/announcing-the-2024-state-of-open-source-report

OpenSSF. (n.d.). Open Source Security Foundation. https://openssf.org/

Shannon, C. (1949). Communication theory of secrecy systems. Bell System Technical Journal, 28(4), 662. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

DIGITAL EURO ASSOCIATION

Digital Euro Association e.V.
Thurn-und-Taxis-Platz 6
60313 Frankfurt am Main

https://www.digital-euro-association.de/

florian.schreiber@digital-euro-association.de

@DigiEuro

Digital Euro Association