Giesecke+Devrient
Creating Confidence

contain

Schlussbericht CONTAIN - Teil II - Eingehende Darstellung

Teilvorhaben: Digitale Währungen

Giesecke+Devrient advance52 GmbH

Dr. Lars Hupel, Markus Bohn, Markus Fischbeck

Public
Released

17.02.2026

Inhalt

Im Rahmen des Vorhabens durchgeführte Arbeiten

Das Teilprojekt der Giesecke+Devrient advance52 GmbH umfasste insgesamt **vier Arbeitspakete mit zwölf Teilarbeitspaketen**, die unterschiedliche inhaltliche Schwerpunkte innerhalb des Gesamtvorhabens abdeckten. Der zentrale Fokus lag dabei auf dem **Arbeitspaket AP-Nr. 4-D „Effiziente Reaktionen durch Serious Games und Analysen“**, das einen wesentlichen Beitrag zur Weiterentwicklung innovativer Trainings- und Analyseansätze leisten sollte.

Im Rahmen dieses Arbeitspakets verantwortete G+D das **Teil-AP-Nr. 4.7 „Digitale Währungen“**. Dieses Teilpaket bildete einen bedeutenden thematischen Schwerpunkt und gliederte sich zur strukturierten Bearbeitung in **neun eigenständige Unter-Arbeitspakete (4.7.1–4.7.9)**. Jedes dieser Unterpakete adressierte spezifische Fragestellungen rund um digitale Währungen, deren Funktionsweise, Risiken und das Zusammenspiel mit sicherheitsrelevanten Szenarien.

Ein weiterer wesentlicher Bestandteil der Arbeiten war die **Analyse von Szenarien potenzieller Cybersecurity-Incidents (AP 2-D Szenaranalyse)** im Kontext digitaler Währungen. Dabei wurden mögliche Angriffswege, Auswirkungen und Reaktionsmechanismen untersucht, um ein fundiertes Verständnis der sicherheitskritischen Herausforderungen zu entwickeln. Diese Analysen erfolgten im **Teilarbeitspaket 2.1 „Identifikation und Beschreibung des Szenars: Angriff einer Ransomware mit Akteuren, Anspruchsgruppen, Prozessen, IT-Infrastruktur und Geschäftsmodelle sowie Threat Vektor“.**

Darüber hinaus leistete G+D **Beiträge zum CONTAIN-Rahmenwerk (AP 3)**, die sicherstellen, dass das Thema digitale Währungen im **CONTAIN-Wiki** fachlich korrekt, umfassend und praxisrelevant abgebildet wird. Dadurch wird das Wissen für alle Projektpartner sowie die Fachöffentlichkeit nachhaltig zugänglich gemacht und in den übergreifenden Projektkontext eingebettet. Die Beiträge erfolgten im Rahmen des Unterarbeitspaketes **3.4 Referenzmodellierung Querschnittsthemen.**

In folgendem Abschnitt werden die wesentlichen Ergebnisse jedes einzelnen Arbeitspaketes aufgeführt. Zudem erfolgt eine Zuweisung der Publikationen zu den betreffenden Arbeitspaketen (siehe nummerierte Liste in Anschluss an diesen Abschnitt).

Arbeitspaket 2 – Szenaranalyse

Im Rahmen des Projekts wurden die funktionalen und technischen Schnittstellen zwischen den entworfenen digitalen Währungen und den Serious Games der beteiligten Konsortialpartner systematisch analysiert und definiert. Ziel dieser Arbeiten war es, ein konsistentes Zusammenspiel zwischen spielerischen Interaktionsmechanismen und den Eigenschaften der digitalen Währungen sicherzustellen. Zu diesem Zweck wurden zunächst die relevanten Spielfunktionen, Belohnungsmechanismen und Nutzerpfade der jeweiligen Serious Games untersucht. Anschließend wurden mögliche Integrationspunkte identifiziert, an denen Zahlungslogiken, Token-Transfers oder Währungsanreize einen echten Mehrwert für das Spielverhalten oder die Lernziele liefern können. Die Ergebnisse dieser Analyse dienten als Grundlage für die spätere Modellierung der Datenflüsse, die Definition von API-Anforderungen sowie die Abstimmung der Sicherheits- und Vertrauensmechanismen der digitalen Währungssysteme mit den technischen Architekturen der Spiele**.**

Darüber hinaus erfolgte eine detaillierte inhaltliche und technische Ausarbeitung der im Projekt dargestellten Anwendungsszenarien, wobei der Fokus auf der sinnvollen Einbettung der digitalen Währungen lag. Dies umfasste sowohl die Analyse der Rollen der verschiedenen Nutzergruppen in den Szenarien als auch die Frage, wie Transaktionen, Incentives oder Währungsevents zur Zielsetzung der jeweiligen Anwendung beitragen. Die digitalen Währungen wurden dabei nicht als isolierte Funktion, sondern als integraler Bestandteil der narrativen und funktionalen Logik der Szenarien betrachtet. In enger Abstimmung mit den Konsortialpartnern wurden verschiedene Ausprägungen der Währungsnutzung — etwa als Belohnungsmechanismus, Motivationsinstrument oder Lernobjekt — bewertet und in die Szenarien integriert. Dieser Beitrag stellte sicher, dass die Szenarien sowohl technisch realistisch als auch pädagogisch beziehungsweise spielmechanisch wirksam gestaltet wurden.

Arbeitspaket 3 – Rahmenwerk

Im Zuge der Weiterentwicklung des projektweiten Rahmenwerks wurden die funktionalen und konzeptionellen Schnittstellen zu den digitalen Währungen systematisch analysiert und

dokumentiert. Ziel dieser Arbeiten war es, sicherzustellen, dass die digitalen Währungen in allen relevanten Architektur-, Prozess- und Interaktionsmodellen des Rahmenwerks angemessen berücksichtigt werden. Dazu gehörte die Prüfung, an welchen Stellen bestehende Komponenten um Mechanismen wie Token Verwaltung, Transaktionsvalidierung oder Sicherheitsanforderungen ergänzt werden müssen. Gleichzeitig wurde untersucht, wie die digitalen Währungen in übergeordnete Strukturen wie Rollenmodelle, Governance-Prozesse und technische Standards des Rahmenwerks eingebettet werden können. Die so identifizierten Schnittstellen bilden die Grundlage für eine konsistente und technisch belastbare Integration der Währungen in das Gesamtsystem und stellen sicher, dass sowohl operative als auch strategische Aspekte des Rahmenwerks mit den Währungsmechanismen harmonieren.

Darüber hinaus wurden konkrete Bausteine für die CONTAIN Toolbox entwickelt und beigetragen, um die im Rahmenwerk erarbeiteten Konzepte technisch nutzbar und für weitere Projektmodule wiederverwendbar zu machen. Diese Bausteine unterstützen insbesondere die modellhafte Einbettung von Währungsmechanismen und erleichtern deren standardisierte Anwendung innerhalb der Gesamtarchitektur.

Ein weiterer zentraler Arbeitsschritt war die strukturierte Integration der digitalen Währungen in das projektinterne Wiki. Hierzu wurden die relevanten Konzepte, technischen Spezifikationen und Anwendungsfälle der digitalen Währungen in verständlicher, nachvollziehbarer Form aufbereitet und in die bestehende Wissensarchitektur eingegliedert. Dies beinhaltete die Erstellung neuer Seiten sowie die Erweiterung bestehender Inhalte, um klar darzustellen, wie die digitalen Währungen in die Projektlandschaft eingebettet sind und wie sie mit anderen Modulen, Rollen oder Prozessen interagieren. Zudem wurden Querverlinkungen zu verwandten Themenbereichen eingebaut, um eine konsistente Navigation und einen schnellen Wissenszugang für alle Projektteilnehmenden zu gewährleisten. Durch diese strukturierte Dokumentation wurde das Wiki zu einer zentralen Referenz für alle Fragen rund um die Gestaltung, Implementierung und Nutzung der digitalen Währungen innerhalb des Projekts.

Arbeitspaket 4.7.1 - Definition von formalen Methoden zur Steigerung der Sicherheit von CBDC-Systemen

Die wesentlichen Ergebnisse dieses Arbeitspaketes sind:

Die Erweiterung formaler Werkzeuge um neue Programmiersprachen

Formale Verifikationssysteme oder Beweisassistenten können um zusätzliche Zielsprachen erweitert werden, sodass aus formalen Spezifikationen ausführbarer Code generiert werden kann. Dies verbessert ihre praktische Anwendbarkeit und erleichtert die Integration formaler Methoden in bestehende Softwareentwicklungsprozesse.

Herausforderungen beim Übergang von funktionalen zu imperativen Sprachen

Wenn eine funktionale, mathematisch orientierte Beschreibungssprache als Grundlage dient, ist die Generierung von Code für imperative Sprachen mit strukturellen Unterschieden verbunden. Insbesondere müssen Konzepte wie algebraische Datentypen, pattern matching, Typklassen oder vergleichbare Abstraktionsmechanismen in der Zielsprache explizit nachgebildet oder durch alternative Sprachkonstrukte emuliert werden.

Extending Isabelle/HOL's Code Generator with support for the Go programming language

Terru Stübinger[1,2] and Lars Hupel[1,2]

[1] Giesecke+Devrient, Prinzregentenstr. 161, 81677 München, Germany
[2] Technische Universität München, School of Computation, Information and Technology, Boltzmannstr. 3, 85748 Garching bei München, Germany
stuebinm@in.tum.de, lars.hupel@tum.de

Abstract. The Isabelle proof assistant includes a small functional language, which allows users to write and reason about programs. So far, these programs could be extracted into a number of functional languages: Standard ML, OCaml, Scala, and Haskell. This work adds support for Go as a fifth target language for the Code Generator. Unlike the previous targets, Go is not a functional language and encourages code in an imperative style, thus many of the features of Isabelle's language (particularly data types, pattern matching, and type classes) have to be emulated using imperative language constructs in Go. The developed Code Generation is provided as an add-on library that can be simply imported into existing theories.

Keywords: Theorem provers · Code generation · Go programming language.

1 Introduction

The interactive theorem prover *Isabelle* of the LCF tradition [14] is based on a small, well-established and trusted mathematical inference kernel written in Standard ML. All higher-level tools and proofs, such as those included in the most commonly-used logic *Isabelle/HOL*, have to work through this kernel.

Many of the tools available to users in *Isabelle/HOL* feel immediately familiar to anyone with experience in functional programming languages: it is possible to define data types, functions, and Haskell-style type classes and instances.

Isabelle's nature as a theorem prover further makes it easy to formalise and prove propositions about such programs. To allow use of such programs outside of the proof assistant's environment, Isabelle comes equipped with a *Code Generator*, allowing users to extract source code in Haskell, Standard ML, Scala, or OCaml, which can then be compiled and executed. This translation of code works by first translating into an intermediate language called *Thingol*, shared between all targets; from this language, code is then transformed into the individual target languages via the principle of *shallow embedding*, that is, by representing constructs of the source language using only a well-defined subset

Publikationen: [1, 3]

Isabelle, ein bekannter Beweis-Assistent, enthält eine funktionale Sprache, die es den Benutzern ermöglicht, Programme zu schreiben und zu analysieren. Bisher konnten diese Programme in einer Reihe funktionaler Sprachen extrahiert werden: Standard ML, OCaml, Scala und Haskell. Diese Publikation erweitert den Code Generator von Isabelle um die Unterstützung der Go-Programmiersprache als fünfte Zielsprache. Im Gegensatz zu den bisherigen Zielsprachen handelt es sich bei Go nicht um eine funktionale, sondern um eine imperative Sprache. Daher mussten viele der Funktionen der Isabelle-Sprache, insbesondere Datentypen, Musterabgleich und Typklassen, mit imperativen Sprachkonstrukten in Go emuliert werden. Die entwickelte Code-Generierung wird als Add-On-Bibliothek bereitgestellt, die einfach in bestehende Theorien importiert werden kann. Die Erweiterung des Code Generators von Isabelle um die Go-Programmiersprache ist ein bedeutender Schritt in der Weiterentwicklung der Programmiersprachenunterstützung.

Arbeitspaket 4.7.2 - Kryptografische Agilität zur adäquaten Reaktion auf Angriffsvektoren aus dem digitalen Raum

Die wesentlichen Ergebnisse dieses Arbeitspaketes sind:

Digitale Währungen hängen zentral von kryptografischen Signaturen ab

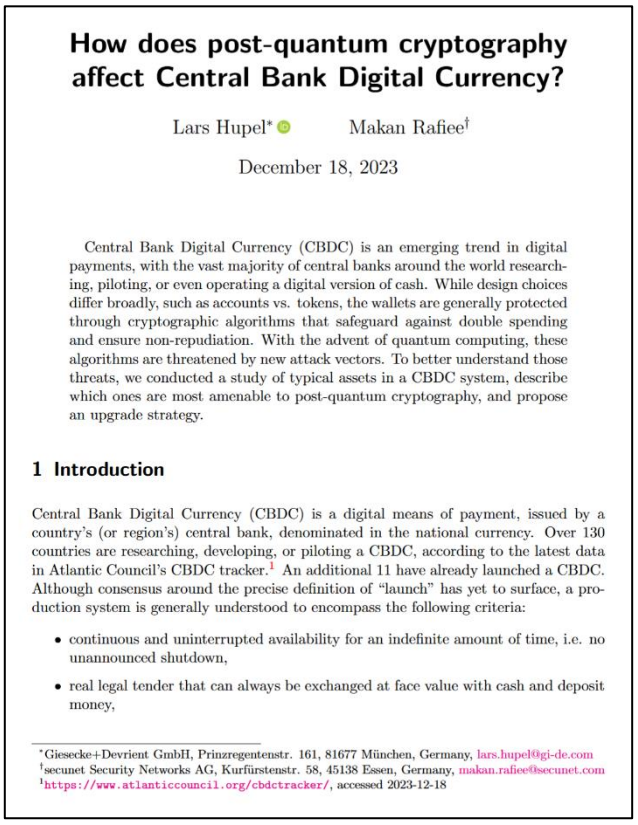
Unabhängig vom konkreten Design digitaler Währungen – ob kontenbasiert oder tokenbasiert – beruhen ihre Sicherheitsmechanismen auf kryptografischen Verfahren. Digitale Wallets verwenden Signaturmechanismen, um:

- Transaktionen zu autorisieren,
- Doppelausgaben zu verhindern,
- Nichtabstreitbarkeit und Integrität sicherzustellen.

Diese Sicherheitsanker sind potenziell anfällig, sobald Quantencomputer in der Lage sind, klassische Signaturverfahren zu brechen.

Quantencomputing erzeugt neue Angriffsvektoren

Viele heute verbreitete Signaturverfahren (z. B. basierend auf RSA oder elliptischen Kurven) sind durch Quantenangriffe – insbesondere Shor's Algorithmus – angreifbar. Daraus entstehen neue Risiken für digitale Währungen, deren Lebenszyklus meist sehr langfristig ausgelegt ist.



How does post-quantum cryptography affect Central Bank Digital Currency?

Lars Hupel* Makan Rafiee†

December 18, 2023

Central Bank Digital Currency (CBDC) is an emerging trend in digital payments, with the vast majority of central banks around the world researching, piloting, or even operating a digital version of cash. While design choices differ broadly, such as accounts vs. tokens, the wallets are generally protected through cryptographic algorithms that safeguard against double spending and ensure non-repudiation. With the advent of quantum computing, these algorithms are threatened by new attack vectors. To better understand those threats, we conducted a study of typical assets in a CBDC system, describe which ones are most amenable to post-quantum cryptography, and propose an upgrade strategy.

1 Introduction

Central Bank Digital Currency (CBDC) is a digital means of payment, issued by a country's (or region's) central bank, denominated in the national currency. Over 130 countries are researching, developing, or piloting a CBDC, according to the latest data in Atlantic Council's CBDC tracker.[1] An additional 11 have already launched a CBDC. Although consensus around the precise definition of "launch" has yet to surface, a production system is generally understood to encompass the following criteria:

- continuous and uninterrupted availability for an indefinite amount of time, i.e. no unannounced shutdown,
- real legal tender that can always be exchanged at face value with cash and deposit money,

*Giesecke+Devrient GmbH, Prinzregentenstr. 161, 81677 München, Germany, lars.hupel@gi-de.com
†secunet Security Networks AG, Kurfürstenstr. 58, 45138 Essen, Germany, makan.rafiee@secunet.com
[1] https://www.atlanticcouncil.org/cbdctracker/, accessed 2023-12-18

Bewertung unterschiedlicher Vermögenswerte eines digitalen Währungssystems

Ein digitales Währungssystem besteht aus verschiedenen Komponenten und Vermögenswerten, die unterschiedlich schützenswert sind, zum Beispiel:

- Schlüssel in Wallets
- Validierungskonten oder Knoten
- Systeminterne Zertifikate
- Offline- oder hardwarebasierte Token
- Back-end-Infrastrukturen

Publikationen: [4, 6]

G+Ds primärer wissenschaftlicher Beitrag in diesem AP [4] befasst sich mit den Auswirkungen von PQC auf digitale Währungen. Deren Gestaltungsmöglichkeiten variieren stark – beispielsweise Konten gegenüber Token – doch in der Regel werden die digitalen Geldbörsen ("wallets") durch kryptografische Algorithmen geschützt. Diese verhindern doppelte Ausgaben und gewährleisten die Unanfechtbarkeit von Transaktionen. Mit dem Aufkommen des Quantencomputings sind diese Algorithmen jedoch neuen Angriffsvektoren ausgesetzt.

Um diese Bedrohungen besser zu verstehen, haben wir eine Studie durchgeführt, in der typische Vermögenswerte in einem CBDC-System untersucht werden. Wir beschreiben, welche davon am besten für die Post-Quantum-Kryptographie geeignet sind und schlagen eine Upgrade-Strategie vor.

Arbeitspaket 4.7.3 - Erhöhung der Sicherheit durch Hardware-Sicherheitsmodule

In diesem AP hat G+D Hardware-Sicherheit für die sicher Abwicklung von CBDC-Zahlungen sowohl online als auch offline untersucht [7]. Im Vergleich zu klassischen Zahlungsverfahren, wie beispielsweise Debit- und Kreditkarten, verfügen tokenisierte Währungen über Offlinefähigkeit und bieten auch die Möglichkeit, Zahlungen direkt zwischen Parteien abzuwickeln. Dies wird von den gängigen Anbietern im Einzelhandel und eCommerce noch nicht unterstützt.

Diese neue Form der Zahlung erhöht die Flexibilität für Kund*innen und Händler*innen, führt dadurch zu stärkerem Wettbewerb und zu sinkenden Kosten. Allerdings entsteht auch eine höhere Komplexität in der Zahlungsabwicklung. Ziel der Studie ist es, ein konzeptuelles

Rahmenwerk zu entwickeln, mit denen CBDC nahtlos in das bestehende Ökosystem eingebunden werden können.

Publikationen: [4, 6, 7]

Arbeitspaket 4.7.4 - Beschränkungen digitaler „Wallets“ zur Steigerung von Sicherheit in digitalen Zahlungssystemen

Die wesentlichen Ergebnisse dieses Arbeitspaketes sind:

Wallet-Designkriterien umfassen funktionale und sicherheitsbezogene Beschränkungen

Digitale Wallets für Zahlungssysteme – unabhängig von ihrer konkreten Implementierung – nutzen häufig Mechanismen wie:

- Transaktions- oder Betraglimits,
- zeitbasierte Beschränkungen,
- periodische Sicherheitsprüfungen oder Health-Checks.

Solche Funktionen dienen allgemein dazu, Risiken zu minimieren, Fehlverhalten frühzeitig zu erkennen und die Gesamtrobustheit des Systems zu verbessern.

Verteilte Schlüsselverwaltung reduziert Single-Point-of-Failure-Risiken

Ein Ansatz zur Absicherung kryptografischer Schlüssel besteht darin, diese nicht an einem Einzelpunkt zu speichern, sondern über mehrere Instanzen oder Geräte zu verteilen. Dadurch lässt sich das Risiko reduzieren, dass ein einzelnes kompromittiertes Gerät oder System vollständigen Zugang zu einem Wallet erhält.

Threshold Signature Schemes (TSS) als etablierter Mechanismus zur gemeinsamen Signaturerstellung

TSS gehören zu den gängigen Verfahren für verteilte Kryptografie. Dabei wird ein privater Schlüssel in mehrere Anteile zerlegt. Eine bestimmte Mindestanzahl von Anteilen (Threshold) wird benötigt, um eine gültige Signatur zu erzeugen. Kein einzelner Teilnehmer kann den Schlüssel rekonstruieren oder eine Signatur allein erzeugen.

Dies unterstützt Systeme, in denen Transaktionen im Konsens mehrerer Instanzen ausgeführt werden müssen.

Publikationen: [5, 7]

Die Publikation [7] befasst sich auch mit bestimmten Designkriterien im Zusammenhang mit Wallet-Beschränkungen, beispielsweise Limits und periodische, automatisierte Sicherheitsprüfungen.

Threshold Signatures for Central Bank Digital Currencies

Mostafa Abdelrahman[1,2], Filip Rezabek[1][0000−0002−9090−5633], Lars Hupel[1,2][0000−0002−8442−856X], Kilian Glas[1], and Georg Carle[1]

[1] Technische Universität München, Munich, Germany
[2] Giesecke+Devrient, Munich, Germany
lars.hupel@tum.de

Abstract. Digital signatures are crucial for securing Central Bank Digital Currencies (CBDCs) transactions. Like most forms of digital currencies, CBDC solutions rely on signatures for transaction authenticity and integrity, leading to major issues in the case of private key compromise. Our work explores threshold signature schemes (TSSs) in the context of CBDCs. TSSs allow distributed key management and signing, reducing the risk of a compromised key. We analyze CBDC-specific requirements, considering the applicability of TSSs, and use Filia CBDC solution as a base for a detailed evaluation. As most of the current solutions rely on ECDSA for compatibility, we focus on ECDSA-based TSSs and their supporting libraries. Our performance evaluation measured the computational and communication complexity across key processes, as well as the throughput and latency of end-to-end transactions. The results confirm that TSS can enhance the security of CBDC implementations while maintaining acceptable performance for real-world deployments.

Keywords: Threshold Signatures · ECDSA · CBDC

1 Introduction

Digital signatures are essential to ensure the authenticity and integrity of online data. They provide a way to verify the origin and integrity of a message, ensuring that the message has not been tampered with and that it indeed comes from the claimed sender. The system's security collapses if the private key sk is compromised, as an attacker could forge signatures. Conversely, if the sk is lost or destroyed, valid signatures cannot be created, leading to availability loss. This overall leads to a single point of failure.

Threshold Signatures Schemes (TSSs) address the vulnerabilities associated with a single point of failure in private key management. The TSS distributes the signing authority among multiple parties, requiring a subset (or threshold t) of these parties to collaborate to produce a valid signature. This trust distribution reduces the risk of key compromise and increases the resilience of the

Mostafa Abdelrahman and Filip Rezabek contributed equally to this paper.

Ferner hat G+D zusätzliche Sicherheitsmaßnahmen von Wallets untersucht [5], wobei der Fokus auf der Verteilung des Schlüsselmaterials lag. Dadurch ist eine Online-Wallet dahingehend eingeschränkt, dass sie nicht mehr autonom, sondern im Konsens mit anderen Instanzen Zahlungen abwickelt. Unsere Arbeit erforscht Threshold Signature Schemes (TSS) im Kontext von CBDCs. TSSs ermöglichen eine verteilte Schlüsselverwaltung, wodurch das Risiko eines kompromittierten Schlüssels verringert wird. Da die meisten aktuellen Lösungen aus Kompatibilitätsgründen auf ECDSA beruhen, untersuchen wir mehrere Threshold ECDSA-Schemata und deren unterstützende Bibliotheken. Die Ergebnisse bestätigen, dass TSS die Sicherheit von CBDC-Implementierungen verbessern kann und dabei eine akzeptable Performance beibehält.

Arbeitspaket 4.7.5 - Erhöhung der Sicherheit von Offline-Zahlungen

Publikationen: [4-7]

Insbesondere die Publikation [4] befasst sich mit der zukünftigen Absicherung der Offline-Zahlungen mit Hinblick auf PQC.

G+D hat weiterhin Beiträge zum ISO-Standard (aktuell in der internationalen Abstimmungsphase) ISO/DIS 13133 geleistet, welches einen besonderen Fokus auf die Sicherheitsanforderungen von Hardware-Wallets legt.

Arbeitspaket 4.7.6 - Sicherheitstechnische Abwägung zwischen Datenschutz und Transparenz

Der Beitrag in diesem Arbeitspaket war eine Analyse einer datenschutzkonformen Erhebung von Endnutzerdaten bei der Durchführung von digitalen Zahlungen. Ziel ist es einerseits sicherzustellen, dass Richtlinien zu Anti Money Laundering (AML) und Counter-Terrorist Financing (CFT) eingehalten werden, andererseits dem Endnutzer aber auch das höchstmögliche Maß an Privatsphäre bei der Zahlungsabwicklung einzuräumen.

Unterschiedliche „information layer" machen es möglich, dass die jeweils relevante Information nicht einer zentralen Einheit bereitgestellt wird, sondern auf verschiedene Akteure aufgeteilt wird – sodass jeder beteiligte Akteur nur die Information bekommt, die zwingend notwendig ist („Need-to-know"-Prinzip).

Arbeitspaket 4.7.7 - Internationale Kompatibilität digitaler Währungen entlang transnationaler Lieferketten

Die wesentlichen Ergebnisse dieses Arbeitspaketes sind:

Es gibt keine One-Size-Fits-All-Lösung für CBDCs

Länder unterscheiden sich stark in wirtschaftlichen, regulatorischen und technologischen Rahmenbedingungen. Daher wird deutlich, dass CBDC-Designs kontextabhängig und flexibel sein müssen. Es existiert kein universelles Modell, das überall gleichermaßen funktioniert.

Retail- und Wholesale-CBDCs erfüllen unterschiedliche Zwecke

Grundsätzlich wird zwischen „Retail CBDC" und „Wholesale CBDC" unterschieden. Erstere ist für individuelle Personen für den Zahlungsverkehr im Alltag zugänglich. Der Fokus liegt auf Endnutzer:innen. Letztere ist für den Interbankverkehr zur Abwicklung großer Transaktionen, Effizienz im Finanzsektor vorgesehen. Beide Varianten bringen jeweils eigene Wertversprechen und technische Anforderungen mit.

Technologische Vielfalt bleibt wichtig

CBDCs können auf verschiedenen technischen Architekturen basieren (DLT, zentralisierte Systeme, hybride Modelle). Das deutet darauf hin, dass die Technologie an Anwendungsfall und nationale Präferenzen angepasst wird.

Interoperabilität ist ein zentraler Erfolgsfaktor

Gerade für grenzüberschreitende Transaktionen und komplexe Lieferketten wird die Interoperabilität zwischen Zahlungssystemen entscheidend. Dies betrifft:

- CBDC-zu-CBDC (verschiedene Länder)
- CBDC-zu-Giralgeld
- CBDC-zu-virtuellen Vermögenswerten (z. B. Stablecoins, tokenisierte Assets)

Länder experimentieren bereits mit grenzüberschreitenden CBDC-Modellen

Es entstehen multilaterale Pilotprojekte, die CBDCs über Ländergrenzen hinweg testen. Parallel dazu nimmt die Integration in breitere digitale Asset-Ökosysteme zu. Die

Ausgestaltung von Interoperabilitäts-Brücken ist hochgradig kontextabhängig. Die Entwicklung von Brücken erfordert:

- detaillierte Analyse der Anwendungsfälle,
- Betrachtung der Stakeholder,
- Bewertung betrieblicher Anforderungen (Sicherheit, Skalierbarkeit, Governance).

Publikation: [2]

Journal of Payments Strategy & Systems Volume 17 Number 4

Interoperability aspects of central bank digital currency across ecosystems and borders

Received (in revised form): 14th November, 2023

Lars Hupel
Chief Evangelist, Giesecke+Devrient, Germany

Lars Hupel

***Lars Hupel** is Chief Evangelist at Giesecke+Devrient. A software engineer with an interest in modern payment services, Lars is frequently invited to public lectures and workshops for banks and central banks to speak on central bank digital currency. Lars is also involved with product development with a primary interest is security, especially the verification of systems using mathematical methods. Lars has also worked as an IT consultant in various industries, including the automotive, blockchain, public transport and data protection sectors. Lars obtained a PhD in informatics in 2019 from the Technical University of Munich.*

Giesecke+Devrient advance52 GmbH, Prinzregentenstraße 161, 81677, München, Germany

Tel: +49 1724891485; E-mail: lars.hupel@gi-de.com

Journal of Payments Strategy & Systems
Vol. 17, No. 4 2023, pp. 422–432
© Henry Stewart Publications, 1750-1806

ABSTRACT

There is a growing consensus that there is no 'one size fits all' central bank digital currency (CBDC). Both retail CBDC and wholesale CBDC have their own unique value propositions and may even be deployed using different technologies. Additionally, some countries are developing multilateral cross-border CBDC solutions, as well as integrations into other digital asset ecosystems, including but not limited to stablecoins, tokenised government bonds and real estate. Although interoperability between different ecosystems is highly desirable, the precise design of such bridges is highly context-dependent and requires careful analysis of use cases, stakeholders and operational concerns. This paper describes the state of the art that has been established in the digital asset community, puts forward some suggestions about the design options relating to CBDC — matching those to potential use cases — and discusses some case studies.

Keywords: central bank digital currency (CBDC), deposit money, stablecoins, real-time gross settlement (RTGS), interoperability, instant payment systems (IPS), cross-border payments

INTRODUCTION

The vast majority of central banks around the world are investigating or piloting a central bank digital currency (CBDC), with a select few already running live systems. Although there is no single universal definition of CBDC as of writing, it is commonly understood to be:

- *A digital representation of a country or region's existing currency*: This means that the CBDC will be denoted in the same currency and be exchangeable at par for other types of money, such as deposit money, in a way that resembles cash;
- *Issued directly by the central bank*: Unlike deposit money and e-money, which are issued by private entities, CBDC represents a direct claim on the issuing central bank, meaning that the central bank has full control over its supply;
- *Usable in electronic payments:* unlike cash, which can only be used for payments in physical proximity, CBDC as digital money can be used both offline and online; and
- *Legal tender*: The ability to use CBDC for any purpose and to discharge monetary obligations.

The Bank for International Settlements (BIS), the international financial body whose membership comprises over 60 central banks, defines CBDC as a 'digital payment

Page 422

Sowohl „retail“ als auch „wholesale“ CBDC haben ihre eigenen einzigartigen Wertangebote und können sogar mit unterschiedlichen Technologien implementiert werden. Gerade mit Hinblick auf transnationale Lieferketten und die Notwendigkeit über Ländergrenzen hinweg digitale Transaktionen durchzuführen verdeutlicht die Relevanz von Interoperabilität zwischen verschiedenen Zahlungssystemen. Einige Länder entwickeln derzeit bereits multilaterale grenzüberschreitende CBDC-Lösungen sowie die Integration in andere digitale Asset-Ökosysteme, wie Stablecoins, tokenisierte Staatsanleihen, Immobilien und anderes.

Allerdings ist die genaue Ausgestaltung solcher Brücken stark kontextabhängig und erfordert eine sorgfältige Analyse der Anwendungsfälle, der Stakeholder und der betrieblichen Belange. Diese Veröffentlichung beschreibt den Stand der Technik, der in der Community für digitale Vermögensgegenstände etabliert wurde. Es werden Vorschläge für die Designoptionen im Zusammenhang mit CBDC vorgelegt, die auf potenzielle Anwendungsfälle abgestimmt sind, und es werden einige Fallstudien diskutiert.

Arbeitspaket 4.7.8 - X.509-Zertifikate für quantencomputerresistente Verfahren zur Steigerung der Resilienz gegen Angriffe aus dem digitalen Raum

Die wesentlichen Ergebnisse aus diesem Arbeitspaket sind:

Eine robuste Public Key Infrastructure (PKI) ist essenziell für CBDC-Systeme

CBDCs benötigen eine große, heterogene Teilnehmerlandschaft (Zentralbanken, Geschäftsbanken, Händler*innen, Kund*innen, Wallet-Provider). Um über alle diese Akteure hinweg Vertrauen, Identität und sichere Kommunikation herzustellen, braucht es eine Public-Key-Infrastruktur (PKI). Historische Vorfälle zeigen: PKI-Misskonfiguration kann systemkritisch sein.

Das Design einer CBDC-PKI erfordert eine Balance zwischen Zentralisierung und

Dezentralisierung

Der vorgeschlagene Grundsatz lautet: „So viel Zentralisierung wie nötig, so viel Dezentralisierung wie möglich." Zentralisierung ist nötig, um den Root of Trust sicher zu verankern und regulatorische Kontrolle zu ermöglichen. Dezentralisierung hingegen vermeidet Single Points of Failure und stellt Skalierbarkeit und Resilienz sicher.

Betriebskontinuität erfordert effektive Mechanismen für Zertifikatswiderruf und -austausch

Zertifikate müssen im laufenden CBDC-Betrieb ausgetauscht oder zurückgezogen werden können, ohne Systemstörungen zu verursachen. Managementprozesse für CRLs, OCSP, Rotationen etc. sind integraler Teil einer funktionierenden CBDC-Sicherheitsarchitektur.

Publikationen: [4, 6]

G+Ds primärer wissenschaftlicher Beitrag in diesem AP [6] befasst sich mit der optimalen Gestaltung einer Public-Key-Infrastruktur (PKI) für CBDC auseinander. Zentralbanken stehen dort vor der Herausforderung, eine Vertrauensbeziehung zu und zwischen der Vielzahl an Teilnehmer*innen aufzubauen, darunter Geschäftsbanken, Händler*innen, Kund*innen und Wallet-Hersteller*innen. Dabei ist eine PKI instrumental. In der Vergangenheit haben Ausfälle von PKI zu erheblichen Schäden geführt. Bereits 2022 erlag der CBDC-Zahlungsverkehr in der Ostkaribischen Währungsunion wegen einer Fehlkonfiguration von Zertifikaten.

How to Design a Public Key Infrastructure for a Central Bank Digital Currency

Makan Rafiee[1] and Lars Hupel[2]
[1]*secunet Security Networks AG, Kurfürstenstr. 58, 45138 Essen, Germany*
[2]*Giesecke+Devrient GmbH, Prinzregentenstr. 161, 81677 München, Germany*
makan.rafiee@secunet.com, lars.hupel@gi-de.com

Keywords: Central Bank Digital Currency, CBDC, Public Key Infrastructure, PKI.

Abstract: Central Bank Digital Currency (CBDC) is a new form of money, issued by a country's or region's central bank, that can be used for a variety of payment scenarios. Depending on its concrete implementation, there are many participants in a production CBDC ecosystem, including the central bank, commercial banks, merchants, individuals, and wallet providers. There is a need for robust and scalable Public Key Infrastructure (PKI) for CBDC to ensure the continued trust of all entities in the system. This paper discusses the criteria that should flow into the design of a PKI and proposes a certificate hierarchy, together with a rollover concept ensuring continuous operation of the system. We further consider several peculiarities, such as the circulation of offline-capable hardware wallets.

1 INTRODUCTION

Central Bank Digital Currency (CBDC) is a digital means of payment, issued by a country's (or region's) central bank, denominated in the national currency. According to the latest results of the annual CBDC survey conducted by the Bank for International Settlements, 94% of the respondents say they are working on digital currency (Di Iorio et al., 2024). As of 2025, many major central banks are pushing forward with CBDC, including the European Central Bank with their *Digital Euro* project.

While many of the projects are not yet in production stage, there is an emerging view that a full launch encompasses at least the following criteria (Hupel and Rafiee, 2024):

- continuous and uninterrupted availability for an indefinite amount of time, i.e. no unannounced shutdown,
- real legal tender that can always be exchanged at face value with cash and deposit money,
- no system resets, i.e. holdings will remain valid,
- upgrade and maintenance work requires little to no intervention from users, except for long-term hardware upgrades, similar to the 2-5 year cycle of bank cards and smartphones.

[a] https://orcid.org/0000-0002-8442-856X

Because CBDC is public digital infrastructure, it needs to satisfy the highest resilience and security standards, at least on par with national settlement and payment systems.

But there are also additional requirements unique to CBDC: As opposed to traditional banking infrastructure, a CBDC would operate in 24/7 mode and has thus very little room for maintenance and/or downtime.

Public Key Infrastructure The backbone of any digital currency is the correct use of cryptographic materials and choosing appropriate security levels. This includes selecting the right algorithms for encryption, key exchange, digital signatures, and hash functions. More succinctly: getting the cryptographic primitives right.

But just picking the right algorithm is not enough to build trust in the whole system. Key material needs to be uniquely and verifiably connected to all entities. Many entities need to be authenticated before payments can happen, for example:

- wallets need to authenticate each other;
- the central bank want to ensure that only authorized wallets are used to hold currency; and
- commercial banks need to confirm that the counterparties they are exchanging money with are genuinely who they claim to be.

Wir schlagen einerseits eine geeignete hierarchische Gestaltung der PKI vor, bei der wir uns auf den Grundsatz „so viel Zentralisierung wie nötig, so viel Dezentralisierung wie möglich" berufen. Andererseits betrachten wir auch die Randaspekte von Zertifikatswiderrufen und -austausch im laufenden Betrieb.

Arbeitspaket 4.7.9 - Identifikation von Anomalien bei digitalen Währungen

Es wurden in einem ersten Schritt grundlegende Überlegung zum Erkennen von und Umgang mit digitalem Falschgeld. Das Ergebnis dieses Teilpaketes bestanden in der Erkenntnis, dass die eigentliche Herausforderung bei der Handhabung der entdeckten Anomalien liegt, die hauptsächlich durch gesetzliche Bestimmungen und Regularien vorgegeben werden muss und weniger in der technischen Umsetzung.

Arbeitspaket 5.3 – Demonstration – Vorbereitung, Durchführung und Analyse der Föderierten Übung

Beitrag zur Föderierten Übung im Februar 2025

Im Rahmen der Föderierten Übung im Februar 2025 entstand ein fachlicher Beitrag, der sowohl die konzeptionellen Grundlagen als auch die praktischen Erkenntnisse aus der Durchführung der Übung aufbereitet. Der Beitrag beschreibt zentrale Herausforderungen, methodische Ansätze sowie erste Ergebnisse aus der Zusammenarbeit der beteiligten Institutionen. Zudem werden Perspektiven für die Weiterentwicklung föderierter Verfahren im Kontext moderner Sicherheits- und Einsatzszenarien aufgezeigt.

Adressierung der Fachöffentlichkeit über die CONTAIN-Gruppe

Zur zielgerichteten Ansprache der einschlägigen Fachöffentlichkeit erfolgt die Veröffentlichung und Diskussion relevanter Inhalte über die Arbeits- und Austauschformate der CONTAIN-Gruppe. Dies umfasst sowohl die Bereitstellung fachlicher Beiträge als auch die aktive Beteiligung an themenspezifischen Diskussionen. Auf diese Weise werden aktuelle Erkenntnisse, Best Practices und methodische Weiterentwicklungen einem spezialisierten Publikum zugänglich gemacht und in den fachlichen Diskurs eingebunden.

Erfolgte Veröffentlichungen der Ergebnisse

1. Terru Stübinger, Lars Hupel: Go Code Generation for Isabelle. *Archive of Formal Proofs, 2024.* https://www.isa-afp.org/entries/Go.html
2. Lars Hupel: Interoperability aspects of CBDC across ecosystems and borders. *Journal of Payments Strategy & Systems, 2023.* https://doi.org/10.69554/MBDJ6710 (full text: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4636197)
3. Terru Stübinger, Lars Hupel: Extending Isabelle/HOL's Code Generator with support for the Go programming language. *Formal Methods, 2024.* https://doi.org/10.1007/978-3-031-71177-0_1
4. Lars Hupel, Makan Rafiee: How does post-quantum cryptography affect Central Bank Digital Currency? *UbiSec, 2023.* https://doi.org/10.1007/978-981-97-1274-8_4 (full text: http://arxiv.org/abs/2308.15787)
5. Mostafa Abdelrahman, Filip Rezabek, Lars Hupel, Kilian Glas, Georg Carle: Threshold Signatures for Central Bank Digital Currencies. *International Workshop on Cryptocurrencies and Blockchain Technology, 2025 (to appear).* https://arxiv.org/abs/2506.23294
6. Makan Rafiee, Lars Hupel: How to design a Public Key Infrastructure for a Central Bank Digital Currency? *SECRYPT, 2025.* https://doi.org/10.5220/0013562300003979 (full text: http://arxiv.org/abs/2412.04051)
7. Lars Hupel: A conceptual model for point-of-sale payment with Retail CBDC. *Journal of Payments Strategy & Systems, 2024*. https://doi.org/10.69554/ETQK2745 (full text: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4912865)

Die wichtigsten Positionen des zahlenmäßigen Nachweises

Die wichtigsten Positionen des zahlenmäßigen Nachweises bilden die Grundlage für eine

transparente und nachvollziehbare Darstellung der eingesetzten Fördermittel. Im Mittelpunkt stehen dabei jene Kostenkategorien, die maßgeblich zur Durchführung des Vorhabens beigetragen haben. Die Förderung umfasste insbesondere die Position **0837 – Personalkosten**, die den Aufwand für projektbezogene Arbeitsstunden und fachliche Leistungen abbilden, sowie die Position **0838 – Reisekosten**, welche alle notwendigen dienstlichen Reisen im Rahmen der Projektumsetzung dokumentiert. Beide Positionen gewährleisten gemeinsam eine strukturierte und prüffähige Aufschlüsselung der Mittelverwendung und sind damit zentraler Bestandteil des zahlenmäßigen Nachweises.

0837 Personalkosten: Dies umfasste sämtliche Arbeitsstunden der Kolleginnen und Kollegen, die für das CONTAIN Projekt gearbeitet haben. Aufgrund der vielschichtigen Aufgliederung des Arbeitspaketes 4.7 in neun verschiedene Teilaspekte, arbeiteten insgesamt 11 Mitarbeiterinnen und Mitarbeiter an dem Projekt. Laut Zuwendungsbescheid nimmt diese Kostenposition einen Anteil von 9% des Budgets ein. Der Schwerpunkt der Arbeiten lag auf dem Arbeitspaket 4.7, welches die effizienten Reaktionen durch Serious Games und Analysen mit Hinblick auf digitale Währungen untersucht.

0838 Reisekosten: Die für das Projekt insgesamt angesetzten Reisekosten belaufen sich laut der Kalkulation des Zuwendungsbescheids auf 6.320,00 €. Bei einer Förderquote von 50% führt dies zu einer Fördersumme für Projektreisen von 3.160,00€. Reisen, die im Rahmen des Projektes angefallen sind, waren vor allem Reisen zu Konferenzen, auf denen die Forschungsergebnisse vorgestellt wurden. Insgesamt wurden Reisen zu sieben Konferenzen bzw. Veranstaltungen mit Zentralbanken gemacht. Die Reiseberichte zu den jeweiligen Reisen wurden per Mail an das VDI Technologiezentrum übermittelt. Zudem wurden Reisen zu den Projekttreffen gemacht. Besonders zu erwähnen ist hierbei das bilaterale Konsortialtreffen in Wien vom 5. März - 6. März 2024. Reisekosten zu den Projekttreffen in München entfielen hingegen aufgrund von wegfallenden Anfahrts- und/oder Übernachtungskosten.

Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten

Der Umfang des Arbeitspakets 4.7, das in die Unterpakete 4.7.1 bis 4.7.9 gegliedert war, machte die Einbindung unterschiedlicher Fachexperten innerhalb der a52 zwingend erforderlich. Die breite thematische Ausrichtung sowie der technische Anspruch der Teilaufgaben ließen sich nur durch die koordinierte Zusammenarbeit von Spezialisten aus den Bereichen Sicherheit, Systemarchitektur, Zahlungsverkehrsprozesse und Qualitätssicherung sachgerecht erfüllen.

Im Verlauf der Projektumsetzung zeigte sich deutlich, dass die ursprünglich angenommene gleichmäßige Verteilung des Arbeitsaufwandes über alle neun Unterpakete nicht realisierbar war. Während zu Projektbeginn eine homogene Aufwandsplanung zugrunde gelegt worden

war, musste diese Annahme aufgrund konkreter technischer Anforderungen und unerwarteter Komplexität einzelner Teilaufgaben angepasst werden. Insbesondere Unterpaket 4.7.5 („Erhöhung der Sicherheit von Offline-Zahlungen“) erwies sich als deutlich umfangreicher als andere Unterpakete. Die Analyse bestehender Sicherheitsmechanismen, die Modellierung potenzieller Angriffsszenarien sowie die Entwicklung neuer Schutzmaßnahmen erforderten wesentlich tiefere Recherchen und umfangreichere Entwicklungszyklen, als es in der ursprünglichen Planung absehbar war. Die Mehraufwände in diesem Bereich waren jedoch sowohl notwendig als auch angemessen, da die Sicherheit offline abgewickelter Transaktionen ein zentraler Erfolgsfaktor für die Gesamtintegrität des Systems darstellt und in direktem Zusammenhang mit regulatorischen und marktseitigen Anforderungen steht. Außerdem flossen die Erkenntnisse in die anderen Unterpakete ein.

Auch die übrigen Arbeiten innerhalb des Arbeitspakets 4.7 waren durch ihren Beitrag zum Gesamtprojekt gerechtfertigt. Die jeweiligen Entwicklungs-, Abstimmungs- und Evaluationsarbeiten waren erforderlich, um die technischen Zielsetzungen des Projekts in voller Breite zu adressieren und sicherzustellen, dass die entwickelten Konzepte praxistauglich, interoperabel und sicherheitskonform umgesetzt werden konnten. Die Flexibilisierung der Ressourcenverteilung im Projektverlauf war daher eine angemessene Reaktion auf die tatsächlichen fachlichen Erfordernisse.

Ein weiterer Bestandteil des Arbeitspaketes war die Dissemination der Projektergebnisse. Dazu gehörte insbesondere die Vorstellung und Diskussion der gewonnenen Erkenntnisse auf internationalen Fachkonferenzen. Insgesamt wurden hierzu sieben Dienstreisen durchgeführt. Diese Aktivitäten dienten nicht nur der Transparenz, sondern auch dem wissenschaftlichen Austausch mit der internationalen Fachcommunity sowie der Validierung der eigenen Forschungsergebnisse im Dialog mit externen Experten. Sämtliche Reiseberichte wurden ordnungsgemäß an das VDI Technologiezentrum übermittelt.

Voraussichtliche Nutzen, insbesondere die Verwertbarkeit des Ergebnisses - auch konkrete Planungen für die nähere Zukunft - im Sinne des fortgeschriebenen Verwertungsplans

Grundlagenforschung für digitale Währungen

Im Rahmen des Projekts wurde vertiefte Grundlagenforschung zu digitalen Währungen betrieben, um deren Funktionsweise, Sicherheit und praktische Einsatzfähigkeit zu verbessern. Durch diese wissenschaftliche Basis leisten wir einen wichtigen Beitrag zur Steigerung der Akzeptanz bei allen relevanten Stakeholdern; darunter Zentralbanken, Geschäftsbanken, Endnutzer, Händler sowie Zahlungsdienstleister. Die gewonnenen Erkenntnisse helfen, Vertrauen aufzubauen und technologische Entscheidungen transparent und fundiert zu untermauern.

Aufbau von Partnerschaften mit interessierten Händlern

Bereits heute bestehen erste Partnerschaften mit Handelsunternehmen, die großes Interesse an unserer Technologie zeigen. Diese Kooperationen ermöglichen es, Anforderungen aus realen Nutzungsszenarien frühzeitig zu berücksichtigen und potenzielle Einsatzfelder praxisnah zu erproben.

Breite Einsetzbarkeit durch standardisierte sichere Hardware

Die Verfügbarkeit sicherer Hardware in Form standardisierter Secure-Element-Technologien ist ein zentraler Faktor für die Skalierbarkeit digitaler Währungen. Da Secure Elements in Smartphones, Wearables, Smartcards und einer Vielzahl von IoT-Geräten verbaut werden können, eröffnet dies eine breite Palette möglicher Anwendungsszenarien.

Ein Beispiel hierfür ist der Festo-Demonstrator für *Machine-to-Machine Payments (M2M)*, der zeigt, wie digitale Währungen in industrielle Prozesse integriert werden können.[1] Ein Konsortium aus DG Nexolution, DZ Bank (beide aus dem Bankensektor), Festo (Industrie) und G+D hat in einem größeren Kontext untersucht, inwiefern maschinelle Prozesse via Pay-per-Use abgerechnet werden können. Ein Industrieunternehmen würde eine Maschine nicht kaufen, sondern von einem Dienstleister mieten. Allerdings wird keine feste monatliche Miete fällig, sondern jede Aktion, beispielsweise Bewegung eines Roboterarms, wird individuell vergütet. Die Herausforderung ist hierbei, dass nicht jede Maschine stets online ist, oder gar über ein „Bankkonto“ verfügt. Wir haben daher unseren Token-basierten Ansatz so adaptiert, dass Maschinen mit individuellen Offline-Wallets ausgestattet werden können. Diese Wallets können dann untereinander autonom Zahlungen, auch im Centbereich, abwickeln.

Verbesserte Resilienz und Identifikation zusätzlicher Forschungsfelder

Durch die Arbeit am Projekt wurden wesentliche Beiträge zur Resilienz digitaler Zahlungssysteme geleistet. Gleichzeitig konnten neue Forschungsansätze identifiziert werden, etwa ein spezieller Crisis Mode, der eine längerfristige Offline-Fähigkeit in Situationen wie Naturkatastrophen oder großflächigen Infrastrukturausfällen sicherstellen soll.

Erkenntnisse über nicht zielführende Arbeitspakete

Im Verlauf des Projekts wurden auch Arbeitspakete identifiziert, die sich als weniger zielführend herausgestellt haben. Hauptsächlich betraf dies Abhängigkeiten von externen Hardwareherstellern, die verlässliche Zeitplanungen erschwerten. Aufgrund dieser externen Faktoren konnten bestimmte technische Ziele des Arbeitspaketes 4.7 nicht innerhalb der geplanten Timelines realisiert werden. Sowohl der Übergabepunkt nach Monat 6 als auch der Meilenstein in Monat 12 wurden allerdings erreicht.

[1] siehe auch https://www.gi-de.com/en/spotlight/trends-insights/enabling-offline-m2m-payments-with-deposit-tokens

Während der Durchführung des Vorhabens dem Zuwendungsempfänger bekannt gewordenen Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Im europäischen Raum ist der „digitale Euro“ der Europäischen Zentralbank das wichtigste Projekt im Bereich der digitalen Währungen. Die EZB legt einen starken Fokus auf Retail-Aspekte wie Offline-Fähigkeit, Hardware-basierte Sicherheit und Zahlungen an POS-Terminals. G+D konnte durch unsere Forschungsarbeit maßgebliche Beiträge zur Gestaltung dieser Aspekte leisten. Aktuell befindet sich die Vorlage zur Regulierung über den digitalen Euro noch beim Gesetzgeber.[2]

Nationale und internationale Komitees und Normungsgremien haben während der Projektlaufzeit zahlreiche Dokumente, zu denen wir beigetragen haben, veröffentlicht. Darunter:

- ISO/DIS 13133 Financial Services — Security Reference Model for Digital Currency Hardware Wallet (SRM-DCHW),[3] planmäßige Veröffentlichung im Laufe von 2026
- ISO/AWI 24982 Digital currencies — Vocabulary,[4] noch in Entwurfsphase
- IMF Fintech Note 2025/005 Technology Solutions to Support Central Bank Digital Currency with Limited Connectivity: A Review of Existing Approaches[5]
- BSI TR-03179-1 und 2 Central Bank Digital Currency Backend und Frontend[6]

Daneben gab es auch weitere Veränderungen im Bezug auf digitale Identitäten, die dieses Projekt nicht direkt, aber zumindest mittelbar betreffen. Durch die Novelle der eIDAS-Verordnung und damit einhergehende Large Scale Pilots (LSPs) wird ein neuer Fokus auf Identitäten auf europäischer Ebene gelegt und die bisherige Strategie weiterverfolgt. Interessant für dieses Projekt und eventuelle weitere Forschungen ist dies in Hinblick auf die Wahrung der Privatsphäre bei gleichzeitiger Sicherstellung eines hohen Vertrauensverhältnisses in Bezahlsituationen.

[2] https://finance.ec.europa.eu/publications/digital-euro-package_en
[3] https://www.iso.org/standard/84287.html
[4] https://www.iso.org/standard/88729.html
[5] https://www.imf.org/en/publications/fintech-notes/issues/2025/08/07/technology-solutions-to-support-central-bank-digital-currency-with-limited-connectivity-a-569259
[6] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03179/TR-03179_node.html