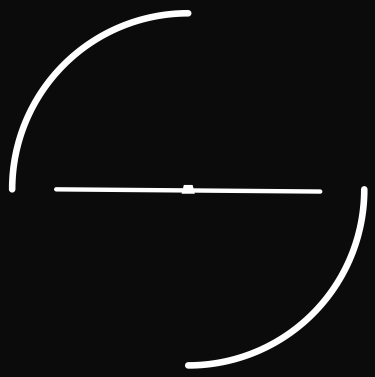


ONOVERA

Das quantensichere Transaktionsverfahren für die nächste Generation digitaler Zahlungen.

PCT-Patent angemeldet – Verfahren zur Absicherung von Zahlungstransaktionen zwischen einem Sender und einem Empfänger

ONOVERA

INHALTSVERZEICHNIS

Diese Übersicht dient als strukturierter Leitfaden durch unsere Präsentation.

Das Problem

Die digitale Zahlungswelt ist nicht auf die Ära der Quantencomputer vorbereitet. Klassische Zahlungskarten und Infrastrukturen basieren auf kryptografischen Verfahren wie RSA oder ECC. Diese gelten als gefährdet durch Algorithmen wie Shor's Algorithmus, sobald leistungsfähige Quantencomputer Realität werden. Darüber hinaus besitzen herkömmliche Smartcards nicht die nötige Rechenleistung, um moderne Post-Quantum-Kryptografie (PQC) wie Falcon-512 oder Kyber effizient umzusetzen. Damit sind Milliarden von Zahlungssystemen potenziell angreifbar. Die Standardisierung von quantensicherer Kryptografie (z. B. durch NIST) schreitet voran – doch eine praktische Integration in Endgeräte bleibt offen.

- Quantencomputer bedrohen RSA & ECC
- Smartcards nicht PQC-fähig
- Bisher kein hardwareseitiger Standard für PQC

Aktuell

- RSA / ECC
- Smartcard (JavaCard)
- Geringe Rechenleistung

Risiko

- Shor-Algorithmus
- Man-in-the-middle möglich
- Keine quantensichere Zukunft

ONOVERA

Unsere Lösung & Vision

Onovera entwickelt ein eigenständiges, sicheres Zahlungsmodul, das speziell für die Integration von Post-Quantum-Kryptografie (PQC) und die Nutzung von Quantum Random Numbers (QRNs) entwickelt wurde. Anstelle der eingeschränkten JavaCard setzen wir auf ein eigenes Modul mit integrierter Hardware, das PQC-Algorithmen wie Falcon-512 nativ verarbeiten kann. Durch die Kommunikation mit einem dedizierten QRNG-Server erhält das Modul quantenzufällige Werte, die Teil des Transaktions-Hashings und der digitalen Signatur werden. Das Ergebnis: Ein vollständig quantensicherer Zahlungsweg, ohne Abhängigkeit von der unsicheren Infrastruktur heutiger Smartcards.

1

Modul empfängt quantenzufälliges k_q

2

Hashing + Signatur mit PQC (Falcon-512)

3

Bank verifiziert Signatur, prüft M = M*

- ✔ Eigenes Modul statt JavaCard
- ✔ Falcon-512 Signaturen lokal
- ✔ Kommunikation mit QRNG-Server
- ✔ Echtzeit-Verifikation durch Bank
- ✔ Kompatibel mit POS & APDU

ONOVERA

Marktchance & Timing

Der Wandel hin zu quantensicherer Kryptografie ist keine Frage des „ob“, sondern des „wann“. Mit der Standardisierung durch das NIST-Post-Quantum-Kryptografie-Projekt entstehen weltweit neue Anforderungen für Zahlungssicherheit – noch bevor Quantencomputer real einsatzbereit sind. Zugleich steigt der regulatorische Druck auf Banken und Zahlungssysteme, sich auf den „Y2Q“-Moment vorzubereiten – also den Tag, an dem Quantencomputer reale Bedrohungen für klassische Kryptografie darstellen.

Warum jetzt der perfekte Zeitpunkt ist:

- Erste NIST-Standards verabschiedet (Kyber, Falcon etc.)
- Banken & Zahlungsdienste benötigen PQC-taugliche Hardware
- Noch kein einheitlicher Hardwarestandard für PQC-Zahlungen verfügbar
- Große Lücke zwischen Forschung & kommerzieller Umsetzung
- Förderprogramme & Investoren suchen nach Post-Quantum-Potenzial

Aktueller Markt

- Klassische Karten & Infrastruktur
- RSA / ECC Kryptografie
- Anfällig für Quantenangriffe
- Geringe Rechenleistung für PQC

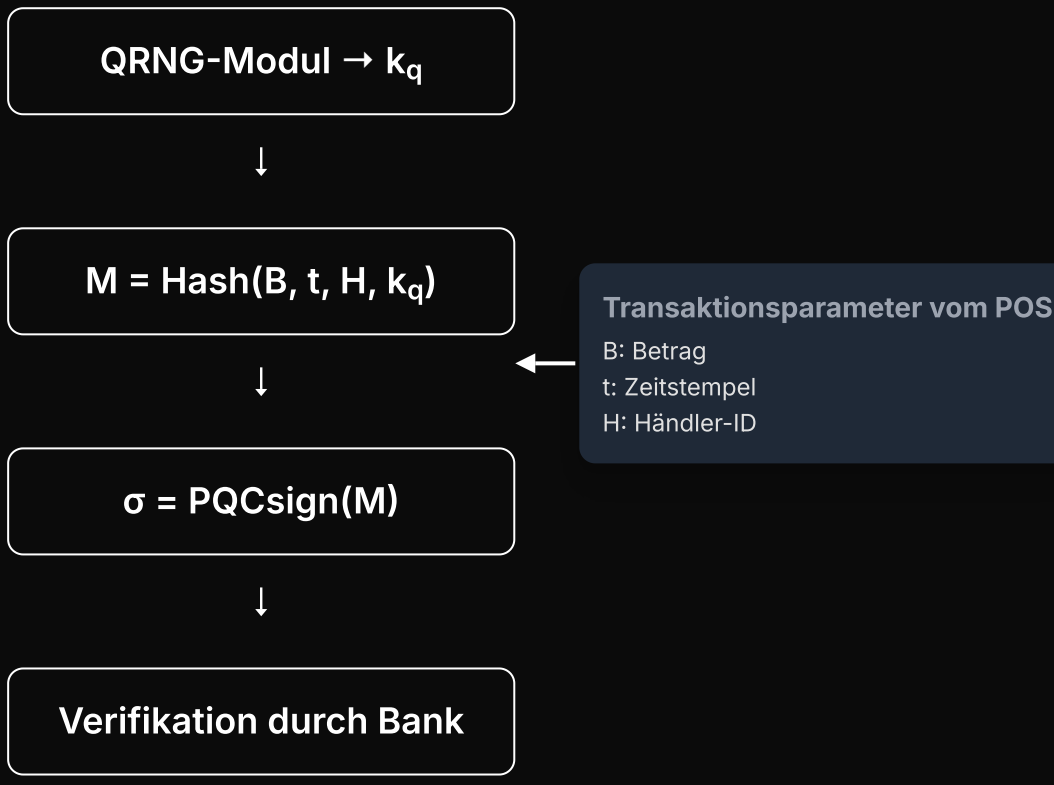
→ Zukunft →

Neuer Markt

- Quantensichere Module
- Falcon & QRNG
- Zukunftssichere Transaktionen
- Hohe Rechenleistung für PQC

ONOVERA

Technologieüberblick – Ablauf der quantensicheren Transaktion



Was passiert hier genau?

Durch die Verbindung einer echten quantenbasierten Zufallszahl mit den Transaktionsdaten entsteht ein einzigartiger Hash-Wert `M`, der jede Transaktion individuell und nicht manipulierbar macht. Dieser wird anschließend mit einem Post-Quantum-Kryptografie-Verfahren signiert.

- Keine Übertragung sensibler Daten – nur die Signatur verlässt das Gerät.
- Fälschungssichere Integrität & Authentizität der Transaktion.
- Kompatibel mit existierenden Bank-APIs und POS-Terminals (APDU/ISO 7816).

ONOVERA

Prototyp – Der erste Funktionsnachweis

Der erste funktionsfähige Prototyp wurde mit einem Raspberry Pi Zero 2W realisiert.

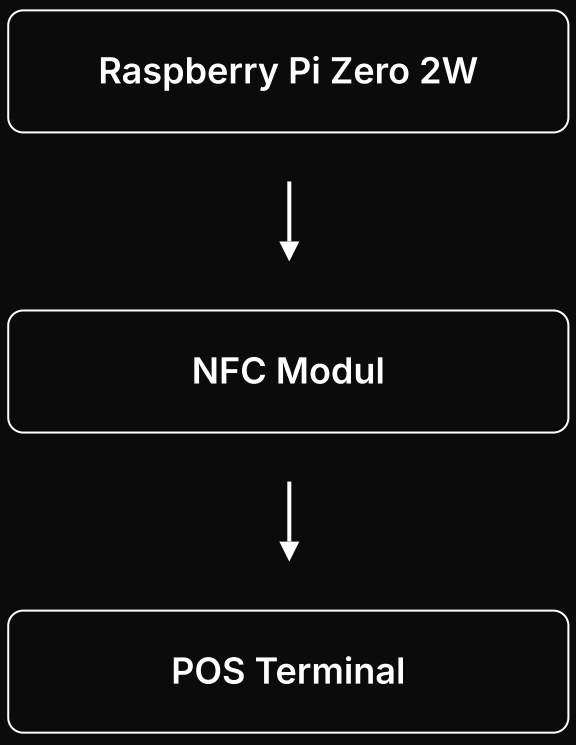
Hauptkomponenten:

- Raspberry Pi Zero 2W mit Linux OS
- NFC-Modul (für APDU-Kommandos vom POS-Terminal)
- WLAN-Verbindung zum lokalen QRNG-Testserver
- Software zur Erzeugung von PQC-Signaturen (Falcon-512)

Funktion:

- Empfang der Transaktionsparameter per NFC
- Abfrage eines quantenbasierten k_q vom QRNG-Testserver
- Hashing + PQC-Signatur lokal am Pi
- Übertragung der Signatur an die simulierte Bankinstanz

Der Prototyp beweist: Das Verfahren kann bereits mit heutigen Kleinstrechnern durchgeführt werden – wenn auch (noch) nicht in Smartcard-Form.



WLAN → Verbindung zum QRNG-Testserver
Falcon-512 → PQC Signatur

ONOVERA

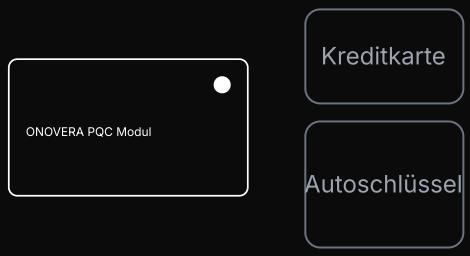
Das zukünftige Modul

Der Prototyp auf Raspberry-Pi-Basis hat bewiesen: unser Verfahren funktioniert. Der nächste Schritt ist die Entwicklung eines eigenständigen, vollwertigen Hardwaremoduls. Es kombiniert Sicherheit, Mobilität und quantenresistente Technologie in einem eleganten, kompakten Format. Das Ziel: ein Produkt, das so einfach mitgeführt werden kann wie eine klassische Bankkarte – aber mit der Sicherheit von morgen.

Technische Merkmale:

- PQC-fähiger Mikrochip (Falcon-512, Dilithium)
- Integriertes Secure Element zur Schlüsselverwaltung
- NFC-Kompatibilität (APDU-Befehle mit POS)
- eSIM-Konnektivität für QRNG-Zugang
- Miniaturisierte kryptografische Recheneinheit (Hash + Signatur)

Formfaktor & Design



Das Modul ist etwas größer als eine klassische Bankkarte, aber dennoch kompakt genug für die Hosentasche oder das Portemonnaie. Weiche Kanten, dezentes Design und optionale Befestigung machen es alltagstauglich.

Anwendung & Vision

Dieses Modul dient als physischer Vertrauensanker für Post-Quantum-Zahlungssysteme. Es ist unabhängig, nicht manipulierbar, offline-signaturfähig – und lässt sich nahtlos in bestehende Infrastruktur integrieren. Ob für Banken, Wallet-Hersteller oder Embedded-Anbieter: ONOVERA bietet die Architektur für sichere Transaktionen im Quantenzeitalter.

ONOVERA

Patent & IP

Das Patent beschreibt ein einzigartiges Verfahren zur quantensicheren Verifikation von Zahlungen, das bereits international als PCT-Patent angemeldet wurde. Es kombiniert Quanten-Zufallszahlen, Hashing und PQC-Signaturen in einer modularen Architektur – optimiert für sichere, offline-fähige Transaktionen.

Schutzumfang:

- Kombination: QRNG + Hashing + PQC
- Synchronisierte Offline-Verifikation
- Architektur der Datenflüsse geschützt
- POS- & Bankkompatibilität abgedeckt
- Erweiterbar für digitale Identität & IoT

IP-Strategie:

Ziel: Internationale Lizenzierung & White-Label-Integration

- Exklusive Lizenzen für Banken & Payment-Netzwerke
- Eigenproduktion zertifizierter Module
- Absicherung gegen Nachbau durch Patente

Das Patent ist der Schlüssel zur Monetarisierung: exklusiv, technologisch führend und wirtschaftlich skalierbar.

ONOVERA

10 – Geschäftsmodell

ONOVERA verfolgt ein skalierbares Geschäftsmodell mit dem Ziel, eine neue Infrastruktur für quantensichere Zahlungssysteme zu etablieren – modular, interoperabel und für Banken & Zahlungsdienstleister lizenziert.

1. White-Label-Lizenzierung

- Lizenzierung des Patents an Banken, Zahlungsnetzwerke & Integratoren
- Integration des PQC-Transaktionssystems in bestehende Systeme
- Customizable SDKs und API-Spezifikationen

2. QRNG as a Service

- Hochsicheres Hosting eigener Quanten-Zufallszahlenserver
- Abrechnung pro Transaktion (Pay-per-RNG)
- Datenschutzfreundlich, auditierbar, EU-gehostet

3. Referenzmodul & Produktion

Die von ONOVERA entwickelte Hardware dient als Blaupause für Zahlungskartenhersteller, FinTechs oder Behörden, um eigene quantensichere Module zu fertigen. Einnahmen erfolgen durch Verkauf oder Lizenz des Designs.

Monetarisierung durch Lizenzierung, Infrastruktur und Vertrauen – ONOVERA wird zur Schlüsseltechnologie für die Ära der Post-Quantum-Zahlungssysteme.

ONOVERA

Go-to-Market & Partner

Onovera verfolgt einen gezielten Markteintritt in Zusammenarbeit mit etablierten Partnern der Zahlungsbranche. Das System wird als White-Label-Modul lizensiert und lässt sich nahtlos in bestehende Zahlungsinfrastrukturen integrieren. Zusätzlich betreiben wir optional eigene QRNG-Server zur sicheren Schlüsselverteilung für Banken, FinTechs oder staatliche Stellen.

Partner-Ökosystem

Kooperation mit Banken, Terminalherstellern, PQC-Anbietern und Regulierungsstellen zur Integration.

White-Label Lizenzierung

Unternehmen können unser Modul & Verfahren in ihr eigenes Ökosystem integrieren.

QRNG Hosting

Wir bieten verifizierte Quanten-Zufallszahlen als unabhängigen Dienst für Banken & Drittanbieter.

Markteintritt

Strategische Pilotprojekte mit Banken & Fintechs zur realitätsnahen Einführung im Zahlungsalltag.

Ziel: Vertrauenswürdige, skalierbare Integration quantensicherer Zahlungstechnologien – gemeinsam mit der Branche.

ONOVERA

Funding & Roadmap

In 18 Monaten zur Lizenzlösung

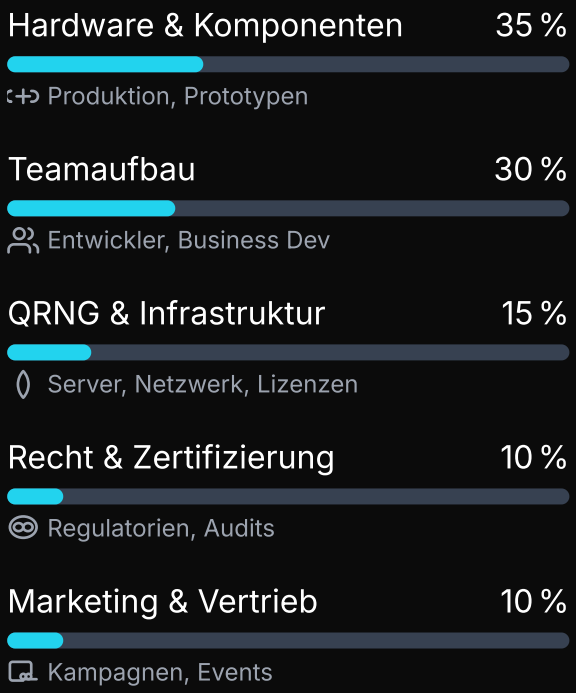
Q3 2025: Startphase
Teamaufbau, Seed-Finanzierung

Q4 2025: Prototyp-Optimierung
Hardware-Miniaturisierung, QRNG-Integration

Q2 2026: Pilotprojekte
Erste Pilotversuche mit Banken & FinTechs

Q4 2026: Lizenzreife
Zertifizierung, Markteinführung & Lizenzierung

Funding Breakdown 1 Mio. €



Ziel: Die vollständig entwickelte, zertifizierte Hardware- und Signatur-Architektur (inkl. QRNG-Anbindung) wird als Lizenzlösung bereitgestellt – mit dokumentiertem Technologiestack und geprüftem Sicherheitskonzept.

Nach erfolgreicher Roadmap-Umsetzung wird ONOVERA das Verfahren als White-Label-Technologie zur Integration in bestehende Zahlungssysteme lizensieren – optional inklusive eigener QRNG-Infrastruktur.

Kontakt & Abschluss

Wir freuen uns darauf, die Zukunft der quantensicheren Zahlungen mit Ihnen zu gestalten.

Founder: Ugurcan Aksoy

E-Mail: kontakt@onovera.com

Website: www.onovera.com

Bereit für die Zukunft?

Sprechen Sie uns an, um mehr über unsere Technologie zu erfahren oder eine Partnerschaft zu besprechen.