DI Dr. Christian Baumann, 9.1.2026 (v0.3)

Automatisierte Notarisierung von Software Artefakten

Git-basierte Workflows liefern lückenlose Versionsnachverfolgung, automatisierte Qualitätsprüfungen und reproduzierbare Builds. Durch die Verknüpfung von Branch-Strategien, CI/CD-Pipelines und Toolchains wird der gesamte Entwicklungs- bis Release-Prozess effizienter und zuverlässiger.

Im Build-Schritt wird für jedes Artefakt ein eindeutiger Hash erzeugt und mittels eines kryptografischen Wallet-Schlüsselpaares in eine Blockchain geschrieben. Der private Schlüssel signiert den Eintrag, der öffentliche Schlüssel ermöglicht die Rückverfolgung des Erstellers. Die dezentrale, unveränderbare Struktur der Blockchain garantiert dauerhafte Integrität, fälschungssicheren Zeitstempel und transparente Herkunftsnachweise – ohne manuelles Eingreifen kann die Notarisierung direkt in Build-Skripte eingebunden werden.

Das Verfahren wird bereits in Österreich über die Austrian Public Service Blockchain (APSB) vom Gesundheitsministerium für eHDSI-Projekte sowie in der Private-Sector-Blockchain (PSBC) von Unternehmen genutzt. Es kombiniert Unveränderbarkeit und Dezentralität mit einer Wallet-basierten Authentifizierung und eignet sich besonders dort, wo Integrität, Nachvollziehbarkeit und zeitliche Dokumentation von Artefakten entscheidend sind.

Beispiel

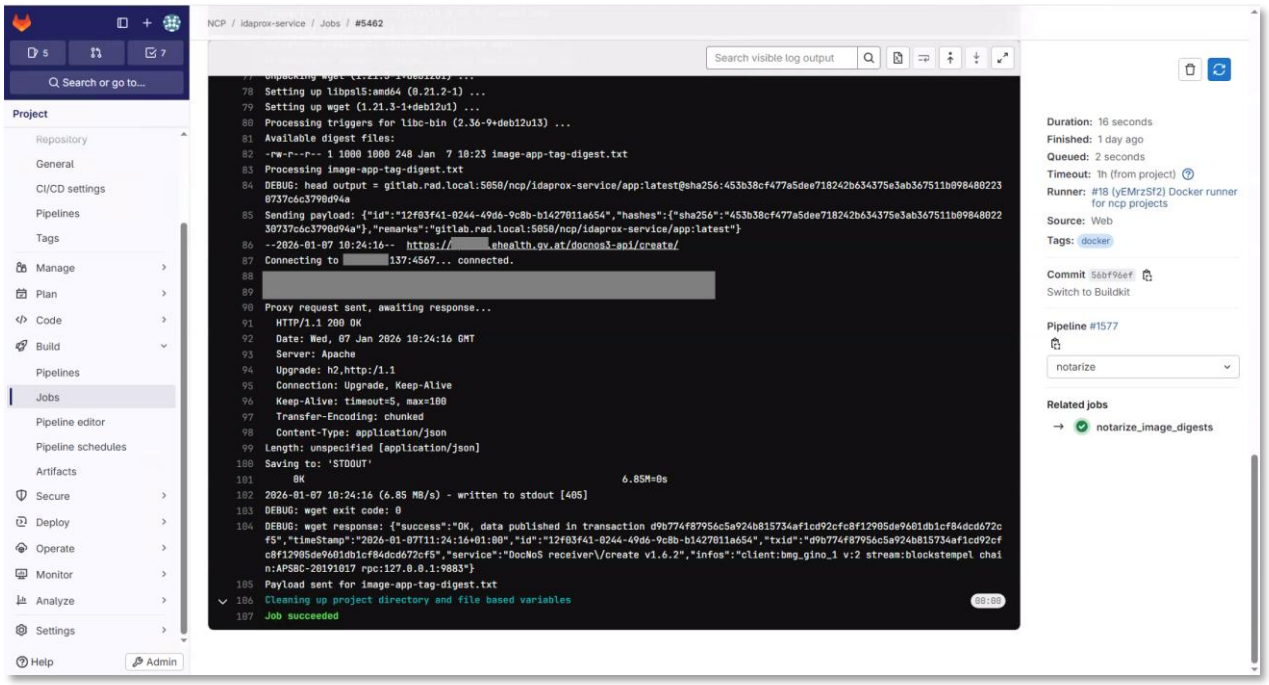

Abbildung 1: Automatischer Aufruf des Notarisierungs-APIs nach Build Success im Build-Job

Publishers	1TMe5s8AHpmQ4j3zjEiH8Jk4A3cx8YTrqjqDHx
Key(s)	Blockstempel-v2 id:12f03f41-0244-49d6-9c8b-b1427011a654 hash:sha256:453b38cf477a5dee718242b634375e3ab367511b0984802230737c6c3790d94a

JSON data	{
	"metadataInternal": {
	"app": "unknown",
	"time": "1767781456000",
	"storageType": "JSON"
	},
	"metadataExternal": {
	"additionalMetadata": null,
	"user": "bmg_gino_1",
	"dataType": "Blockstempel-v2",
	"tags": [
	"Blockstempel-v2",
	"id:12f03f41-0244-49d6-9c8b-b1427011a654",
	"hash:sha256:453b38cf477a5dee718242b634375e3ab367511b09848022307
	]
	},
	"data": {
	"id": "12f03f41-0244-49d6-9c8b-b1427011a654",
	"time": "2026-01-07T11:24:16+01:00",
	"hashes": {
	"sha256": "453b38cf477a5dee718242b634375e3ab367511b0984802230737
	},
	"optional": {
	"size": null
	}
	}
	}

Added	2026-01-07 10:24:26 GMT (confirmed)

Abbildung 2: Proof in der Blockchain (TimeStamp/Blocktime, Hashwert und Metadaten

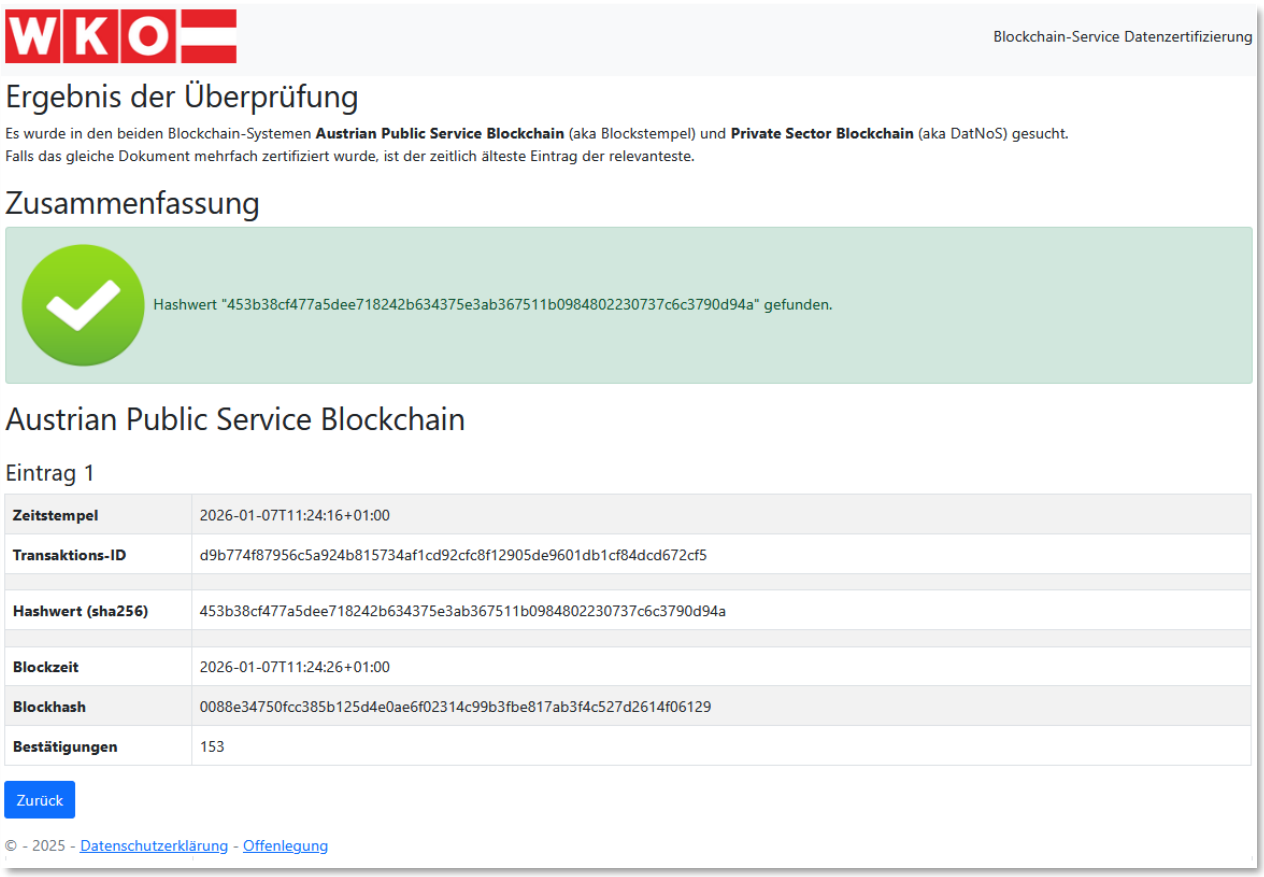

Abbildung 3: Verifikation über Web-GUI - am Beispiel https://daten-zertifizierung.at

Automatisierte Notarisierung von Software Artefakten (Detaillierte Version)

Git-basierte Workflows bieten nahtlose Versionsnachverfolgbarkeit, automatisierte Qualitätsprüfungen und reproduzierbare Builds, wodurch der gesamte Entwicklungs- bis Release-Prozess gestrafft wird. Durch die enge Verknüpfung von Branch-Strategien, CI/CD-Pipelines und Toolchains erreichen Teams höhere Effizienz, Zuverlässigkeit und eine schnellere Auslieferung von Software.

Im Build-Prozess dient die Notarisierung von Software-Artefakten der Sicherstellung von Integrität und Nachvollziehbarkeit. Traditionell erfolgt dies durch das Signieren der Artefakte mithilfe kryptografischer Verfahren. Die Signatur belegt, dass das Artefakt aus einer bestimmten Quelle stammt und unverändert ist. Solche Signaturen erfüllen oft regulatorische und plattformspezifische Anforderungen.

Mit dem Einsatz einer Blockchain verändert sich der Ansatz der Notarisierung. Nach dem Build wird für jedes Artefakt ein eindeutiger Hashwert erzeugt, der anschließend in eine Blockchain eingetragen wird. Hierbei ist zu beachten, dass ein solcher Eintrag ohne Signatur nicht möglich wäre: Um in die Blockchain zu schreiben, benötigt man ein Wallet, das mit einem kryptografischen Schlüsselpaar verknüpft ist. Der Eintrag des Hashwerts in die Blockchain wird mithilfe des privaten Schlüssels des Wallets signiert. Der öffentliche Schlüssel, der dem Wallet zugeordnet ist, ermöglicht es, die Herkunft des Blockchain-Eintrags nachzuvollziehen und weist auf den Ersteller der Notarisierung des Artefakts hin.

Die Blockchain sorgt mit ihrer dezentralen und unveränderbaren Struktur für die dauerhafte Sicherung und Nachvollziehbarkeit dieser Einträge. Eine Überprüfung lässt sich jederzeit durchführen, indem der aktuelle Hash eines Artefakts mit dem gespeicherten Wert in der Blockchain verglichen wird. Dieses Verfahren dokumentiert Integrität und Zeitpunkt eindeutig und fälschungssicher.

Das Blockchain-basierte Verfahren bietet Vorteile wie Unveränderbarkeit, Dezentralität und Transparenz. Es ersetzt zwar nicht in allen Fällen die klassische Herausgeber-Authentifizierung über dedizierte Zertifikatsstellen, führt aber dank Wallet-basiertem Schlüsselpaar den Nachweis, wer eine Notarisierung vorgenommen hat. Geeignet ist dieses Modell insbesondere dort, wo die Integrität, der Zeitstempel und die nachvollziehbare Zuordnung der Artefakte im Mittelpunkt stehen.

In Österreich kommt dieses Verfahren bereits im Rahmen der Austrian Public Service Blockchain (APSB) zum Einsatz. Das Gesundheitsministerium (BMASGPK) nutzt es beispielsweise für Softwareprojekte, die mit der eHDSI (eHealth Digital Service Infrastructure) verbunden sind.

Auch im Umfeld der Private Sector Blockchain (PSBC) greifen verschiedene Unternehmen auf diese Methode zurück.

Die technische Umsetzung dieser Automatisierung basiert darauf, dass zunächst die Hashwerte der erzeugten Artefakte berechnet werden. Anschließend erfolgt ein Aufruf eines Blockchain-APIs, um die Hashwerte in die Blockchain zu übertragen. Dieser Vorgang lässt sich nahtlos in Build-Skripte integrieren, wie sie in Git-basierten Systemen üblich sind. Dadurch wird die Notarisierung direkt im Rahmen des Build-Prozesses durchgeführt und erfordert kein manuelles Eingreifen.