

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-Schlüsselpaars 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 Herkunftsnnachweise – 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

The screenshot shows a build log interface for a project named 'idprox-service'. The log output window displays the following command sequence:

```
77 unpacking wget (1.11.0-1+deb12u1) ...
78 Setting up libpopt5:amd64 (0.21.2-1) ...
79 Setting up wget (1.11.0-1+deb12u1) ...
80 Processing triggers for libc-bin (2.36-9+deb12u13) ...
81 Available digest files:
82 -rw-r--r-- 1 1000 1000 248 Jan 7 16:23 image-app-tag-digest.txt
83 Processing image-app-tag-digest.txt
84 DEBUG: head output = gitlab.rad.local:5059/ncp/idprox-service/app:latest@sha256:453b38cf477a5dee718242b63437Se3ab367511b098480223
85 Sending payload: {"id": "12f03f41-0244-49d6-9c8b-b1427011a654", "hashes": {"sha256": "453b38cf477a5dee718242b63437Se3ab367511b098480223", "digest_type": "sha256"}, "remarks": "gitlab.rad.local:5059/ncp/idprox-service/app:latest"}
86 --2026-01-07 10:24:16-- https://health.gv.at/docnos3-api/create/
87 Connecting to 137.45.67... connected.
88
89
90 Proxy request sent, awaiting response...
91 HTTP/1.1 200 OK
92 Date: Wed, 07 Jan 2026 10:24:16 GMT
93 Server: Apache
94 Upgrade: h2; http/1.1
95 Connection: Upgrade, Keep-Alive
96 Keep-Alive: timeout=5, max=100
97 Transfer-Encoding: chunked
98 Content-Type: application/json
99 Length: unspecified [application/json]
100 Saving to: 'STDOUT'          6.85M=0s
101
102 2026-01-07 10:24:16 (6.85 MB/s) - written to stdout [405]
103 DEBUG: wget exit code: 0
104 DEBUG: wget response: {"success": "OK, data published in transaction d9b774f87956c5a924b815734ef1cd92fcf8f12905de9601db1cf84dd672c
105 f5", "timeStamp": "2026-01-07T11:24:16+01:00", "id": "12f03f41-0244-49d6-9c8b-b1427011a654", "txid": "d9b774f87956c5a924b815734ef1cd92fcf
106 c8f12905de9601db1cf84dd672c5", "service": "DocNoS_receiver@create v1.6.2", "infos": "client:bmg_gino_1 v:2 stream:blockstempel chai
107 n:APSB-20191017 rpc:127.0.0.1:9883"}
108 Payload sent for image-app-tag-digest.txt
109 Cleaning up project directory and file based variables
110 Job succeeded
```

The log concludes with 'Job succeeded'. The interface also shows various project settings like pipelines, tags, and artifacts, along with pipeline details and related jobs.

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

Publishers	1TMe5s8AHpmQ4j3z EiH8Jk4A3cx8YTrjqjDHx
Key(s)	Blockstempel-v2 id:12f03f41-0244-49d6-9c8b-b1427011a654 hash:sha256:453b38cf477a5dee718242b634375e3ab367511b0984802230737c6c3790d94a
JSON data	<pre>{ "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:sha256:453b38cf477a5dee718242b634375e3ab367511b0984802230737c6c3790d94a"] }, "data": { "id": "12f03f41-0244-49d6-9c8b-b1427011a654", "time": "2026-01-07T11:24:16+01:00", "hashes": { "sha256": "453b38cf477a5dee718242b634375e3ab367511b0984802230737c6c3790d94a" }, "optional": { "size": null } } }</pre>
Added	2026-01-07 10:24:26 GMT (confirmed)

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

Ergebnis der Überprüfung

Es wurde in den beiden Blockchain-Systemen **Austrian Public Service Blockchain** (aka Blockstempel) und **Private Sector Blockchain** (aka DatNoS) gesucht.
Falls das gleiche Dokument mehrfach zertifiziert wurde, ist der zeitlich älteste Eintrag der relevanteste.

Zusammenfassung



Hashwert "453b38cf477a5dee718242b634375e3ab367511b0984802230737c6c3790d94a" gefunden.

Austrian Public Service Blockchain

Eintrag 1

Zeitstempel	2026-01-07T11:24:16+01:00
Transaktions-ID	d9b774f87956c5a924b815734af1cd92fcf8f12905de9601db1cf84dcfd672cf5
Hashwert (sha256)	453b38cf477a5dee718242b634375e3ab367511b0984802230737c6c3790d94a
Blockzeit	2026-01-07T11:24:26+01:00
Blockhash	0088e34750fcc385b125d4e0ae6f02314c99b3fbe817ab3f4c527d2614f06129
Bestätigungen	153

[Zurück](#)

© - 2025 - [Datenschutzerklärung](#) - [Offenlegung](#)

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.