Showcase „Zeugnisvalidierung über Blockchains“

Digital-Gipfel | 12. Juni 2017 | Innovation Lab

Motivation

"Frisierte" Zeugnisse nehmen vor dem Hintergrund steigender Bewerberzahlen deutlich zu […]. Die Einschätzungen von Fachdetekteien und Personalchefs zum Anteil solcher Manipulationen reichen vom Promillebereich bis zu einem Drittel. Fälschungen werden dabei nicht nur bei Arbeitszeugnissen, sondern auch bei Schul-, Ausbildungs- und Hochschulzeugnissen […] beobachtet.

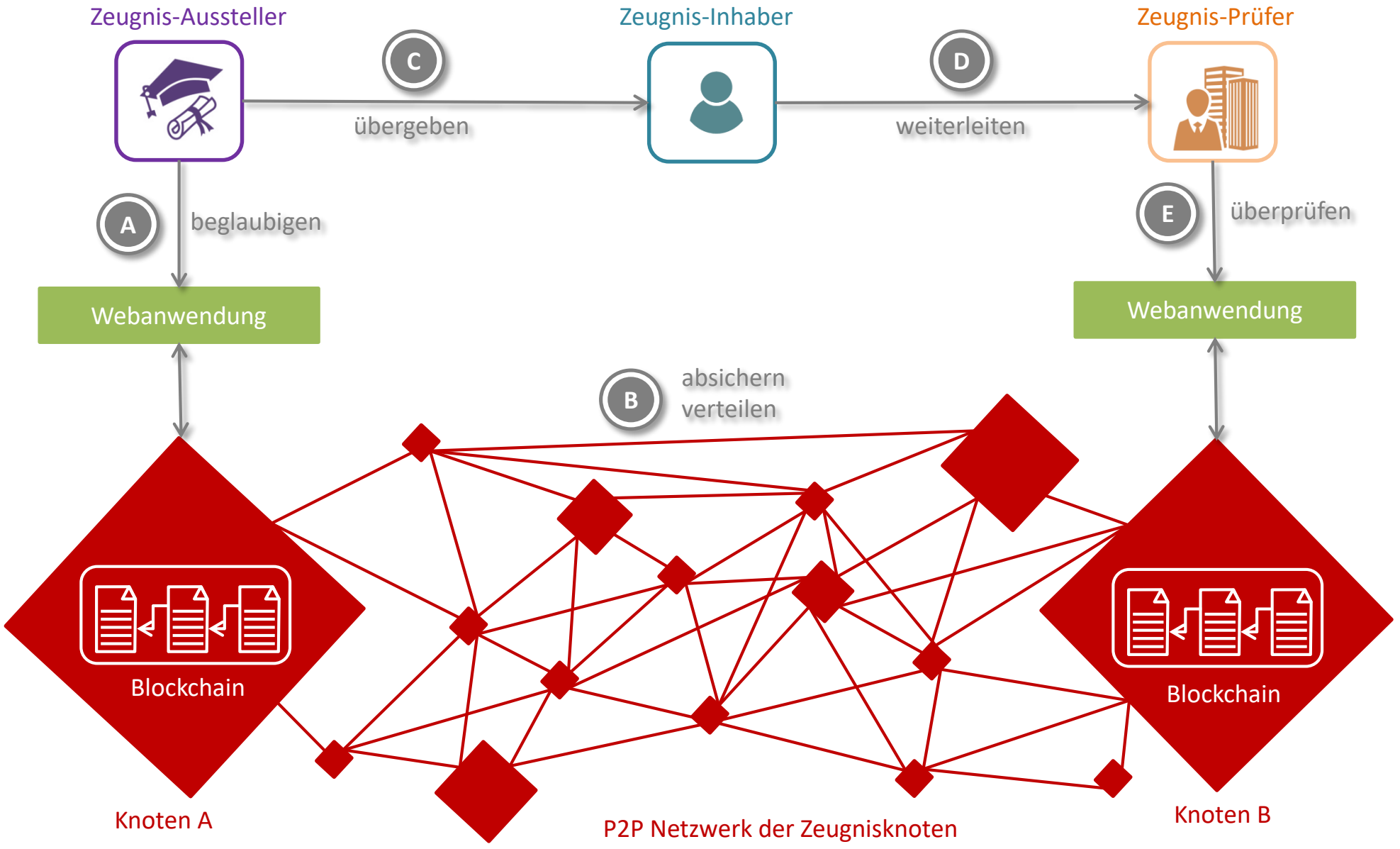
http://www.sicherheitsmelder.de/xhtml/articleview.jsf;jsessionid=A605A6ACCE91E9B94828BED9207A1A53.BoorbergSolrAppLive?id=4776E3BFCC9A.htm

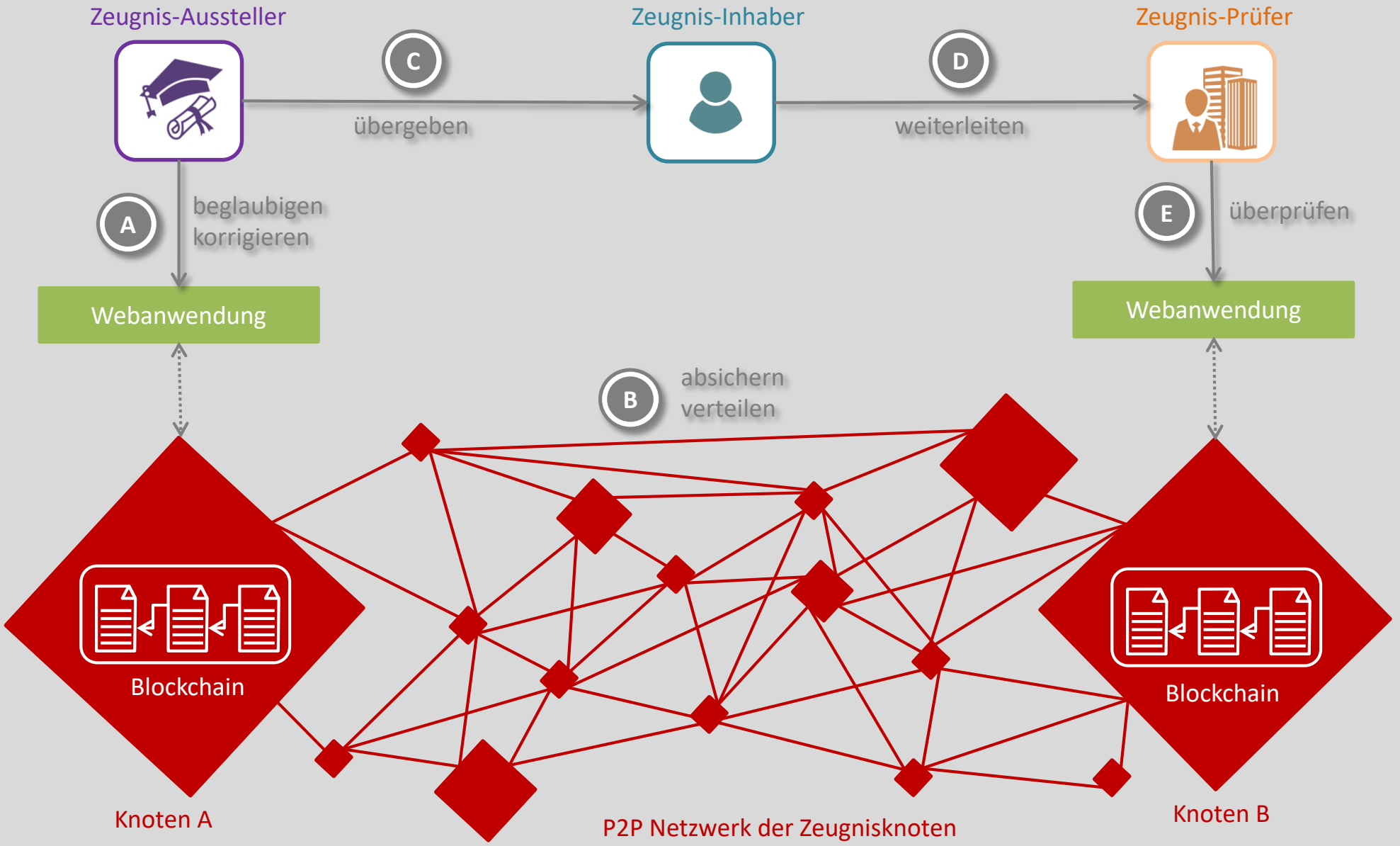
Blockchain zur Zeugnisvalidierung - Merkmale

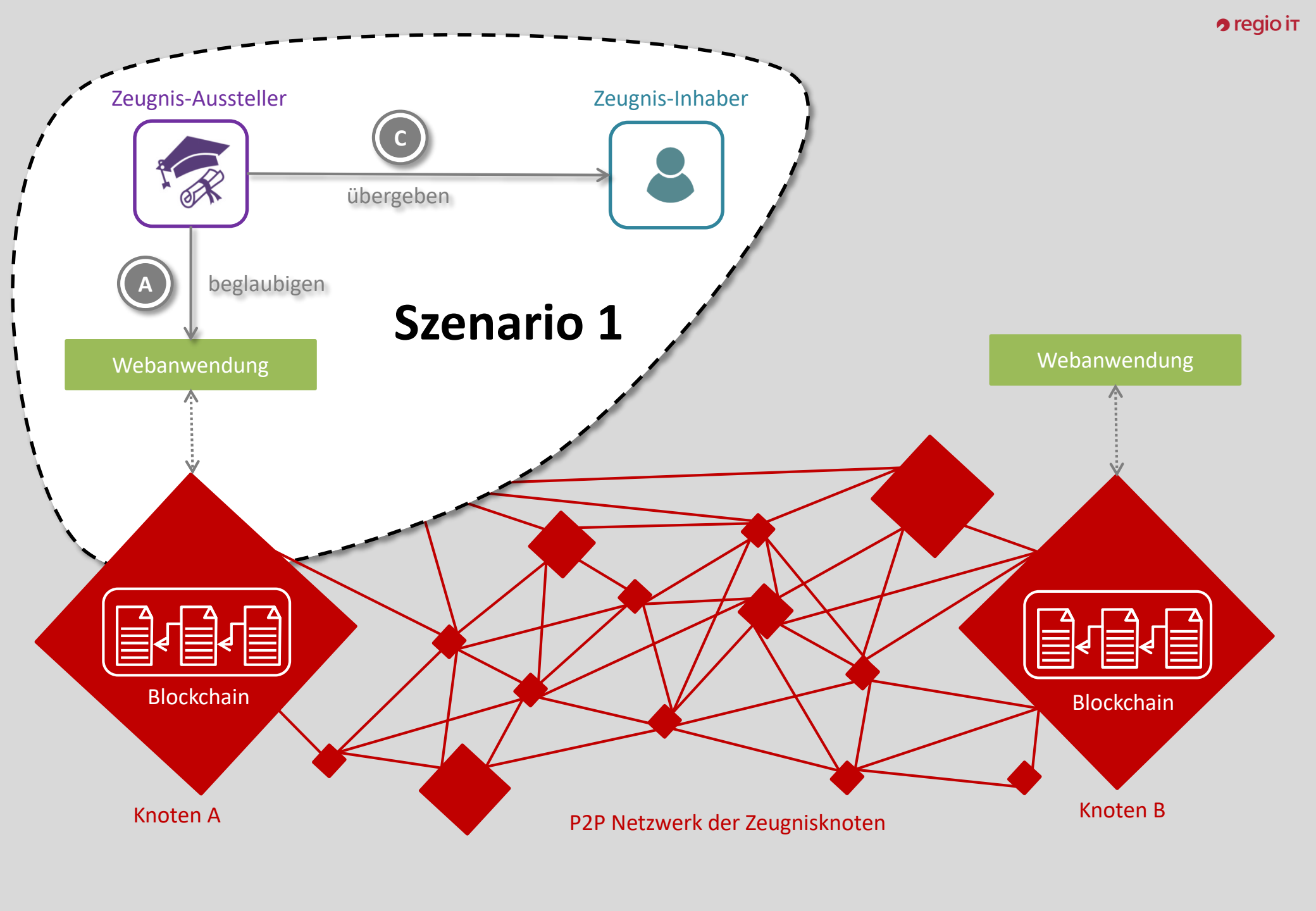
- Designentscheidung ausschließlich für Demonstrator
- Validierung von Zeugnissen anhand der Speicherung von Signaturen.
- Private Blockchain:
  - Knoten bei allen für die Ausstellung von Zeugnissen autorisierten Institutionen.
  - Schreiben von Signaturen nur durch diese Institutionen.
  - Lesen anonym und öffentlich.
- Korrekturen mit Hilfe von „Stornoeinträgen“ .

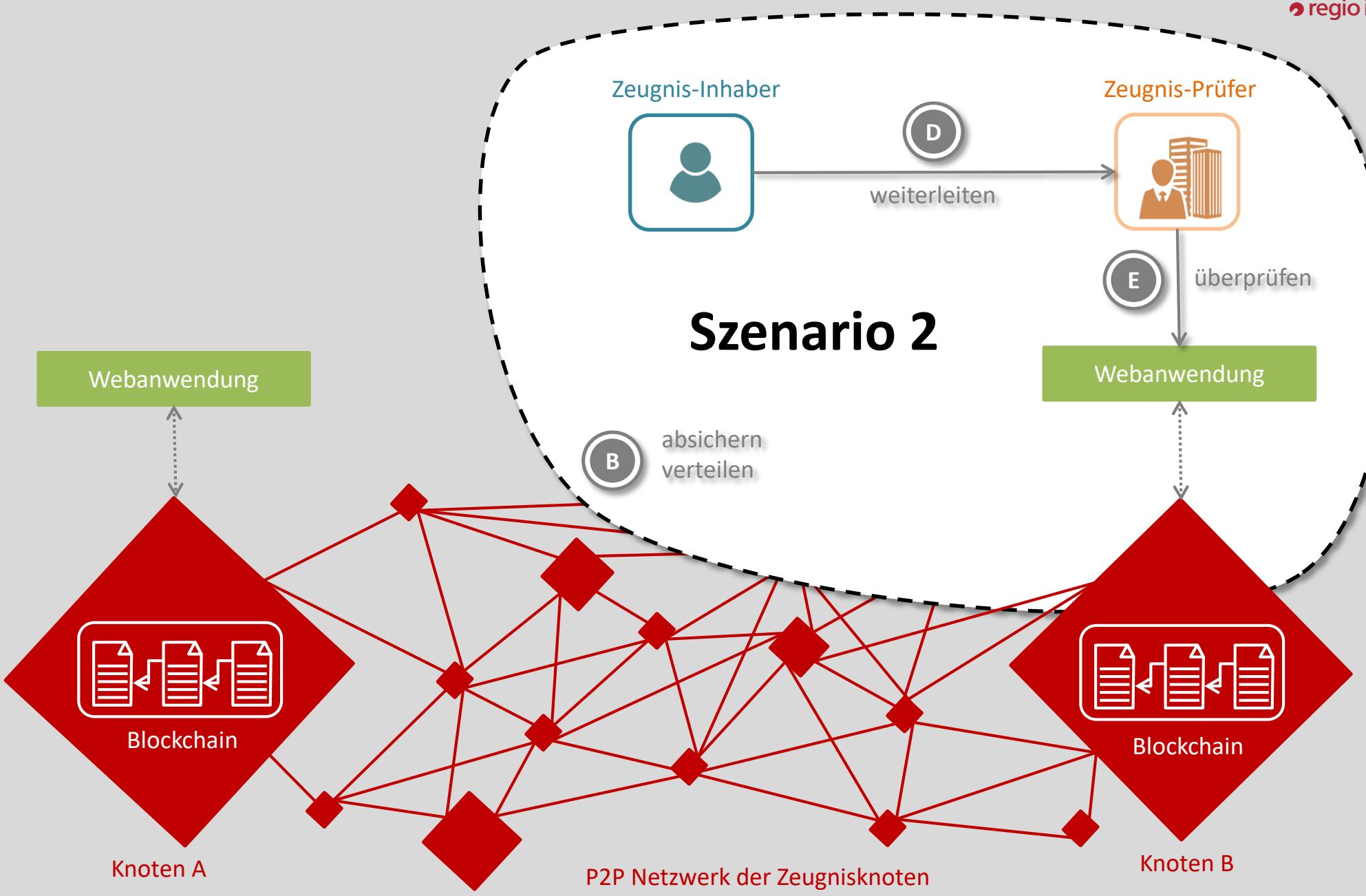
Warum Blockchain zur Zeugnisvalidierung?

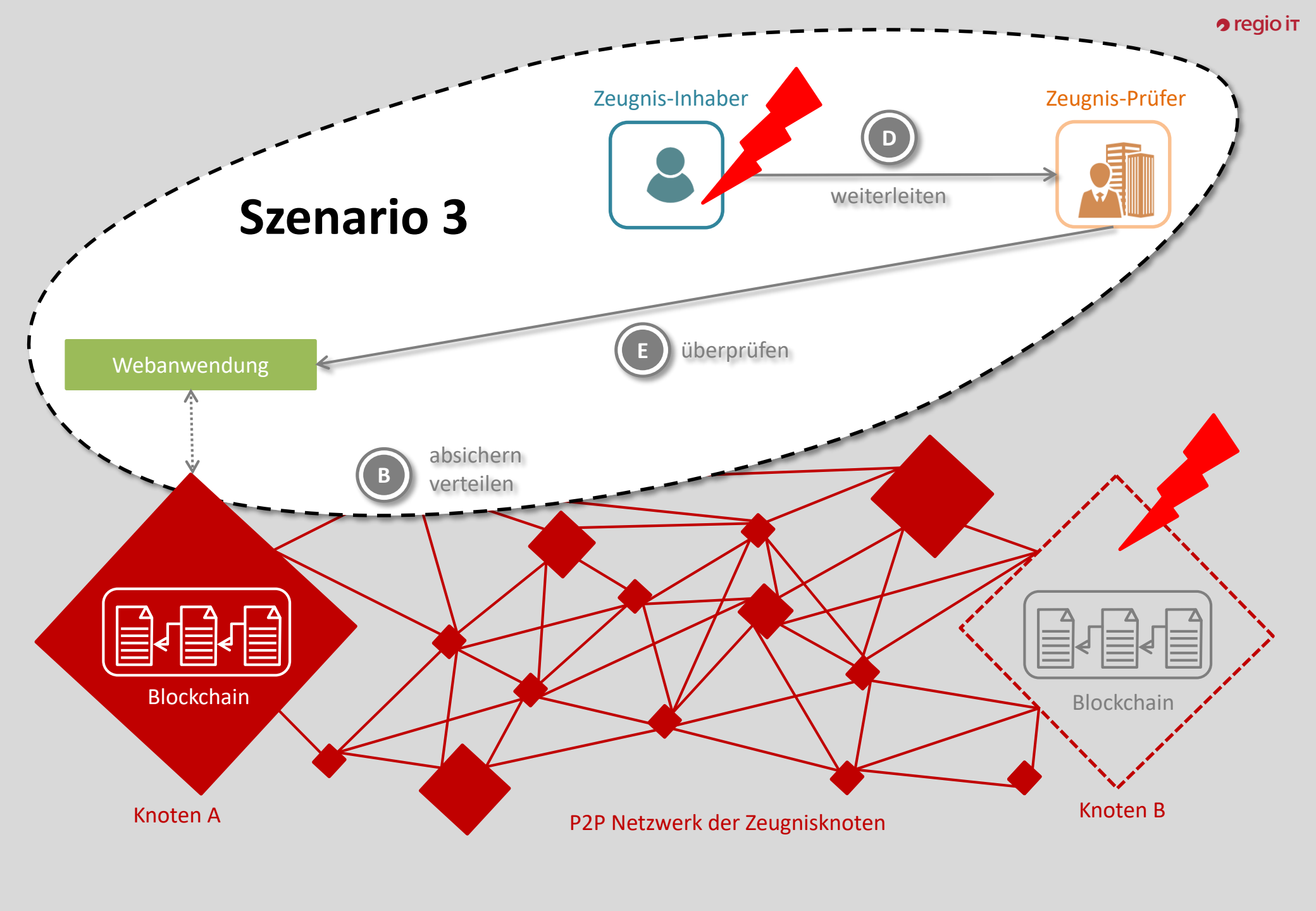
- Verteilt – Distributed
  - Hochverfügbar…wie das Internet.
  - Skalierbarkeit, z.B. bei steigender Anzahl der Verifikationsanfragen.
  - Kein Betreibermonopol, jeder kann am Konzept partizipieren.
  - Ausfallsicherheit und implizites Backup.
- Öffentlich verifizierbar, jeder kann lesen und auf Korrektheit prüfen.
- Irreversibel, nicht manipulierbar.

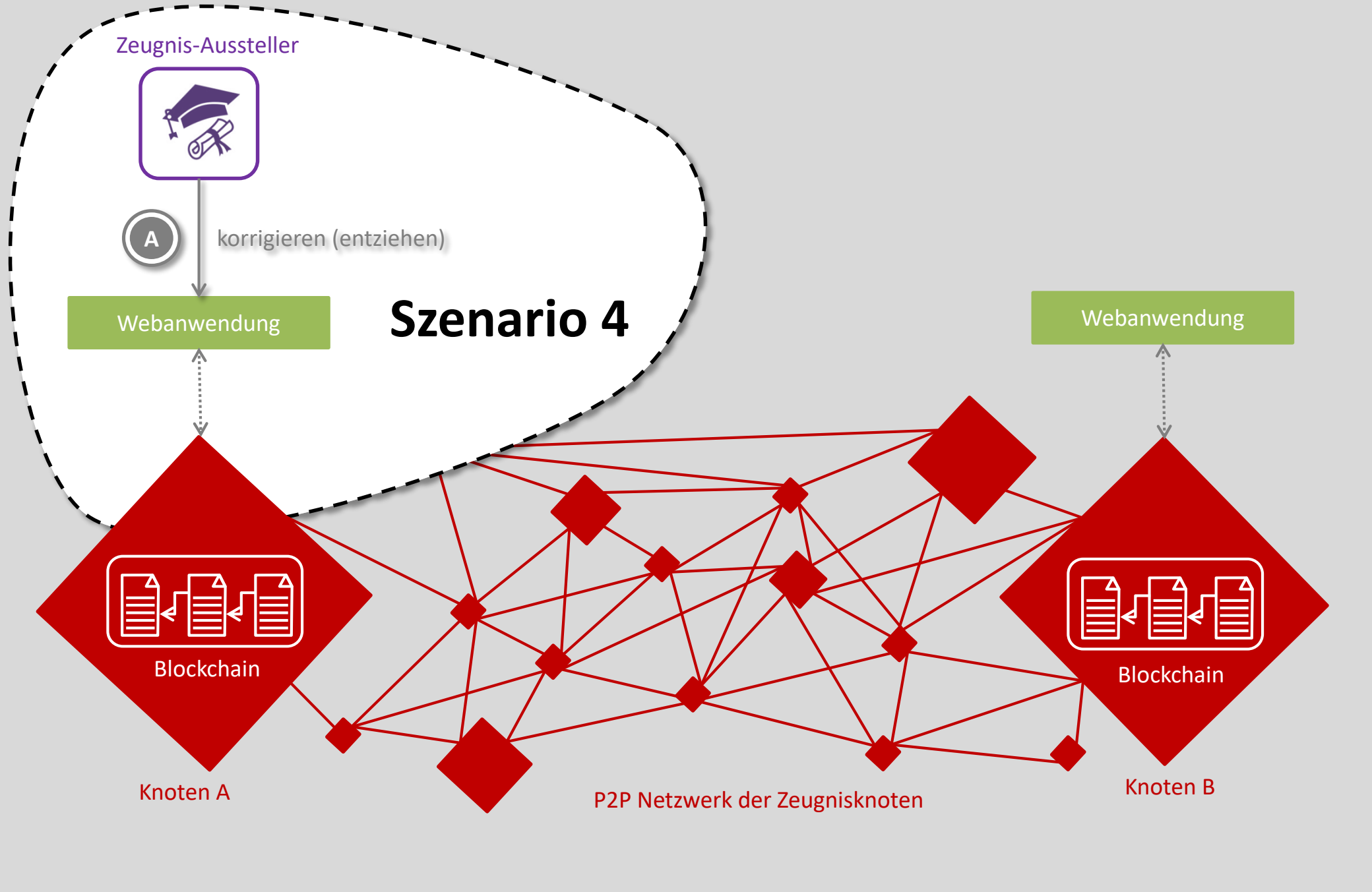

Zeugnis-Aussteller
Zeugnis-Inhaber
Zeugnis-Prüfer
C
übergeben
D
weiterleiten
A
beglaubigen
E
überprüfen
Webanwendung
Webanwendung
B
absichern
verteilen
Blockchain
Blockchain
Knoten A
P2P Netzwerk der Zeugnisknoten
Knoten B

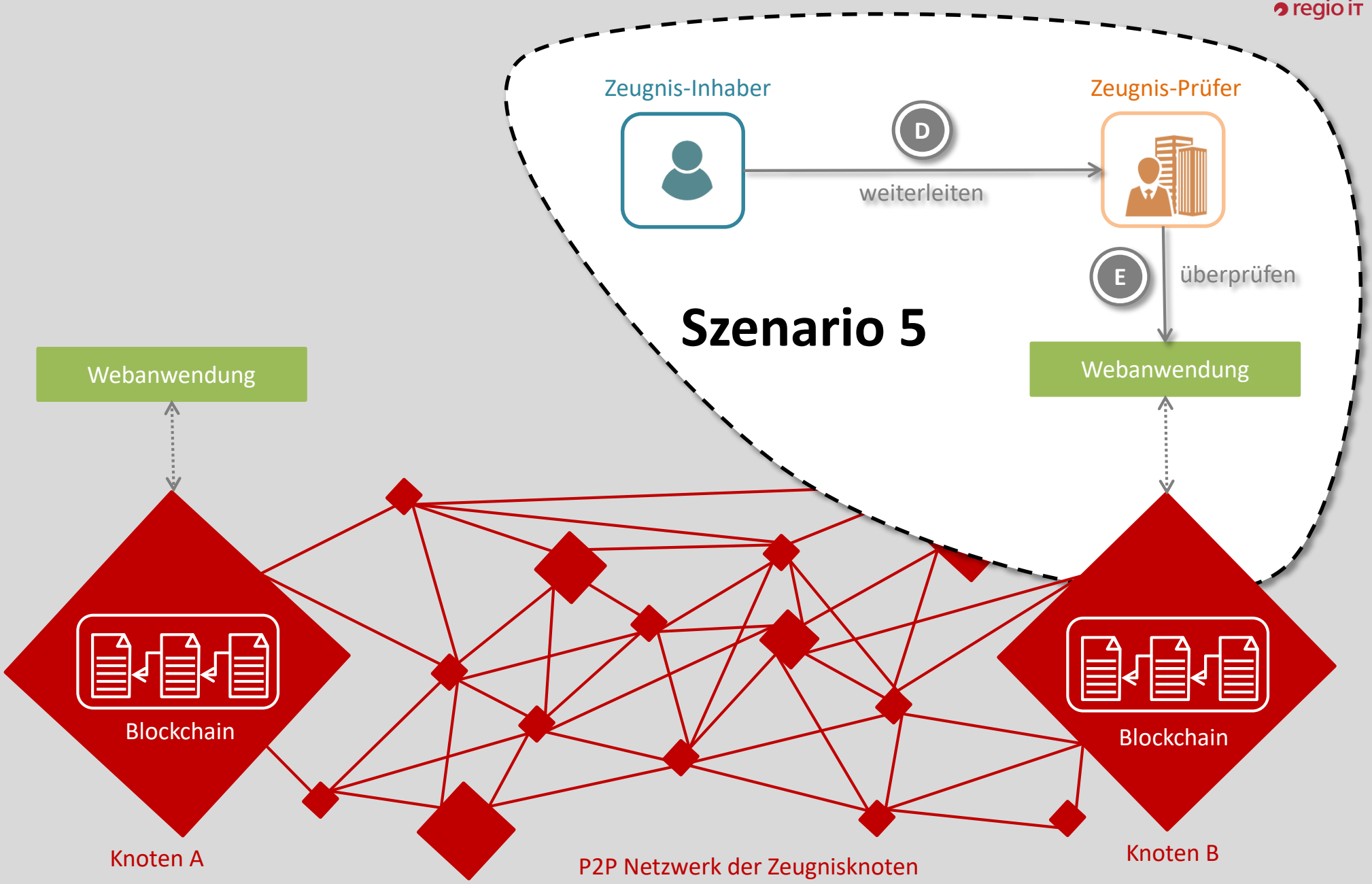

Zeugnis-Aussteller
Zeugnis-Inhaber
Zeugnis-Prüfer
C
übergeben
D
weiterleiten
A
beglaubigen
korrigieren
E
überprüfen
Webanwendung
Webanwendung
B
absichern
verteilen
Blockchain
Blockchain
Knoten A
P2P Netzwerk der Zeugnisknoten
Knoten B


Zeugnis-Aussteller
Zeugnis-Inhaber
C
übergeben
A
beglaubigen
Szenario 1
Webanwendung
Webanwendung
Blockchain
Blockchain
Knoten A
P2P Netzwerk der Zeugnisknoten
Knoten B


Zeugnis-Inhaber
D
weiterleiten
Zeugnis-Prüfer
E
überprüfen
Szenario 2
Webanwendung
Webanwendung
B
absichern
verteilen
Blockchain
Blockchain
Knoten A
P2P Netzwerk der Zeugnisknoten
Knoten B


Szenario 3
Zeugnis-Inhaber
Zeugnis-Prüfer
D
weiterleiten
E
überprüfen
Webanwendung
B
absichern
verteilen
Blockchain
Blockchain
Knoten A
P2P Netzwerk der Zeugnisknoten
Knoten B

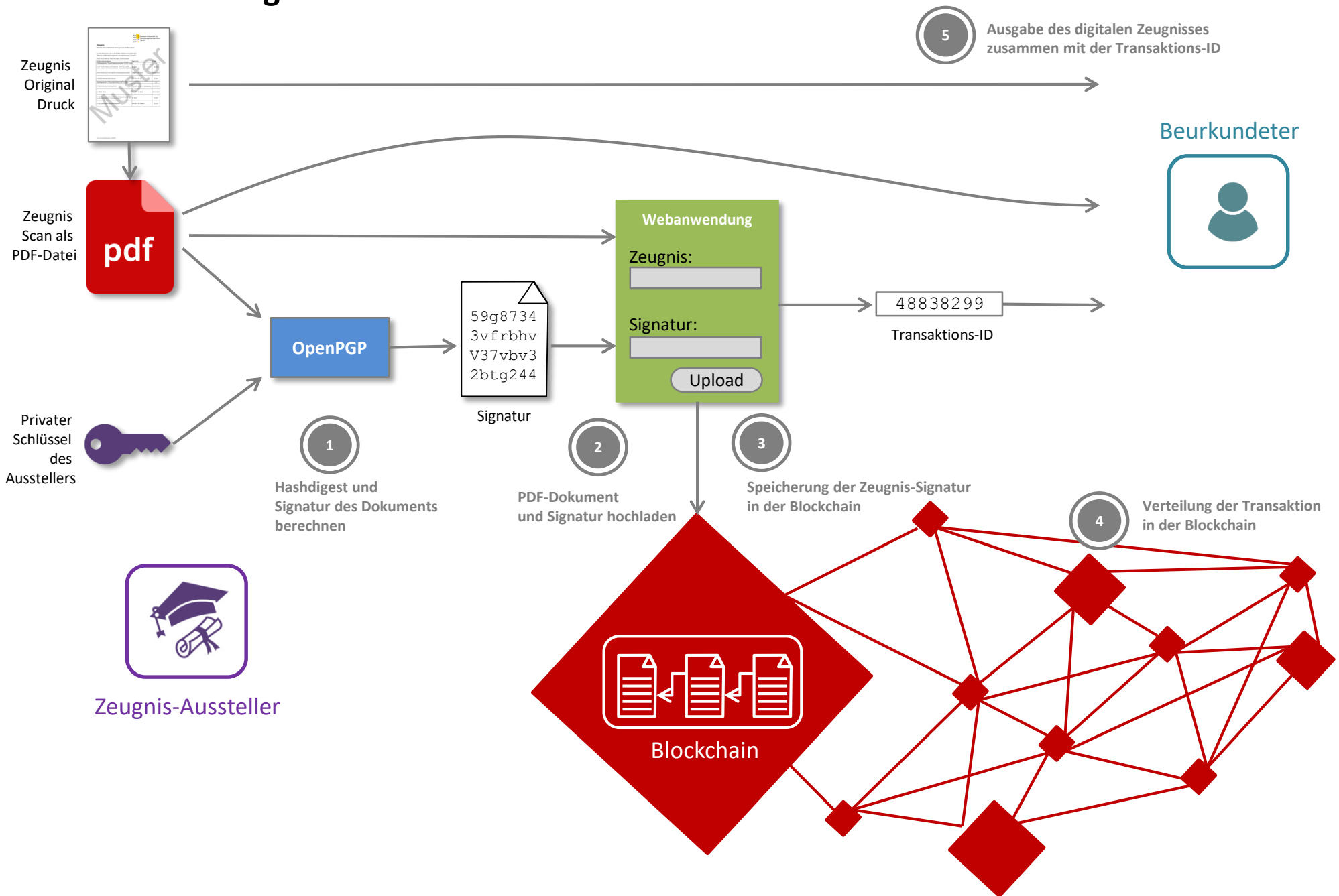

Zeugnis-Aussteller
A
korrigieren (entziehen)
Webanwendung
Szenario 4
Webanwendung
Blockchain
Blockchain
Knoten A
P2P Netzwerk der Zeugnisknoten
Knoten B


Zeugnis-Inhaber
D
weiterleiten
Zeugnis-Prüfer
E
überprüfen
Szenario 5
Webanwendung
Webanwendung
Blockchain
Blockchain
Knoten A
P2P Netzwerk der Zeugnisknoten
Knoten B

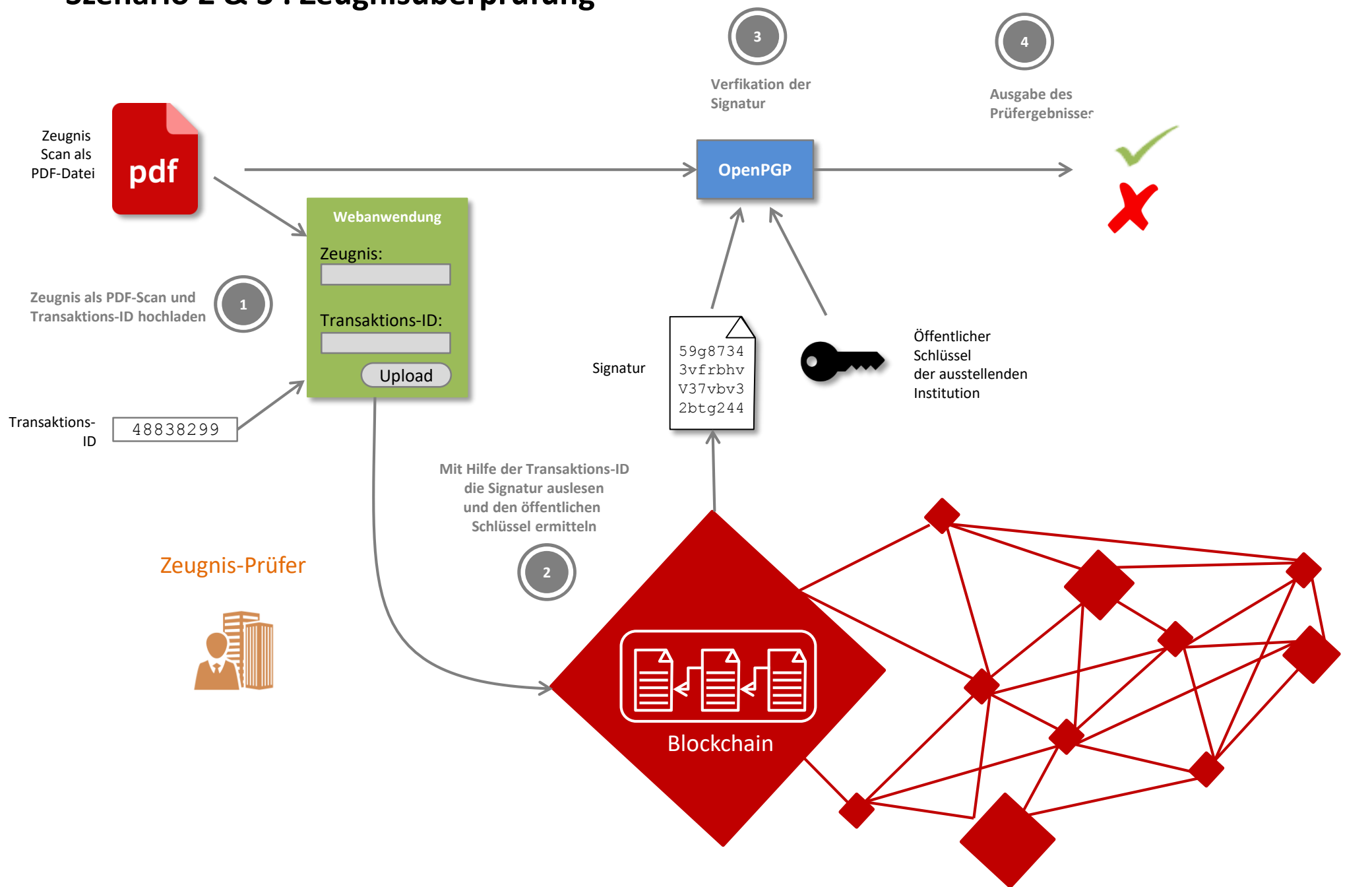
Herzliche Einladung zur Diskussion…

Technische Zusatzinformationen zu den Szenarien…

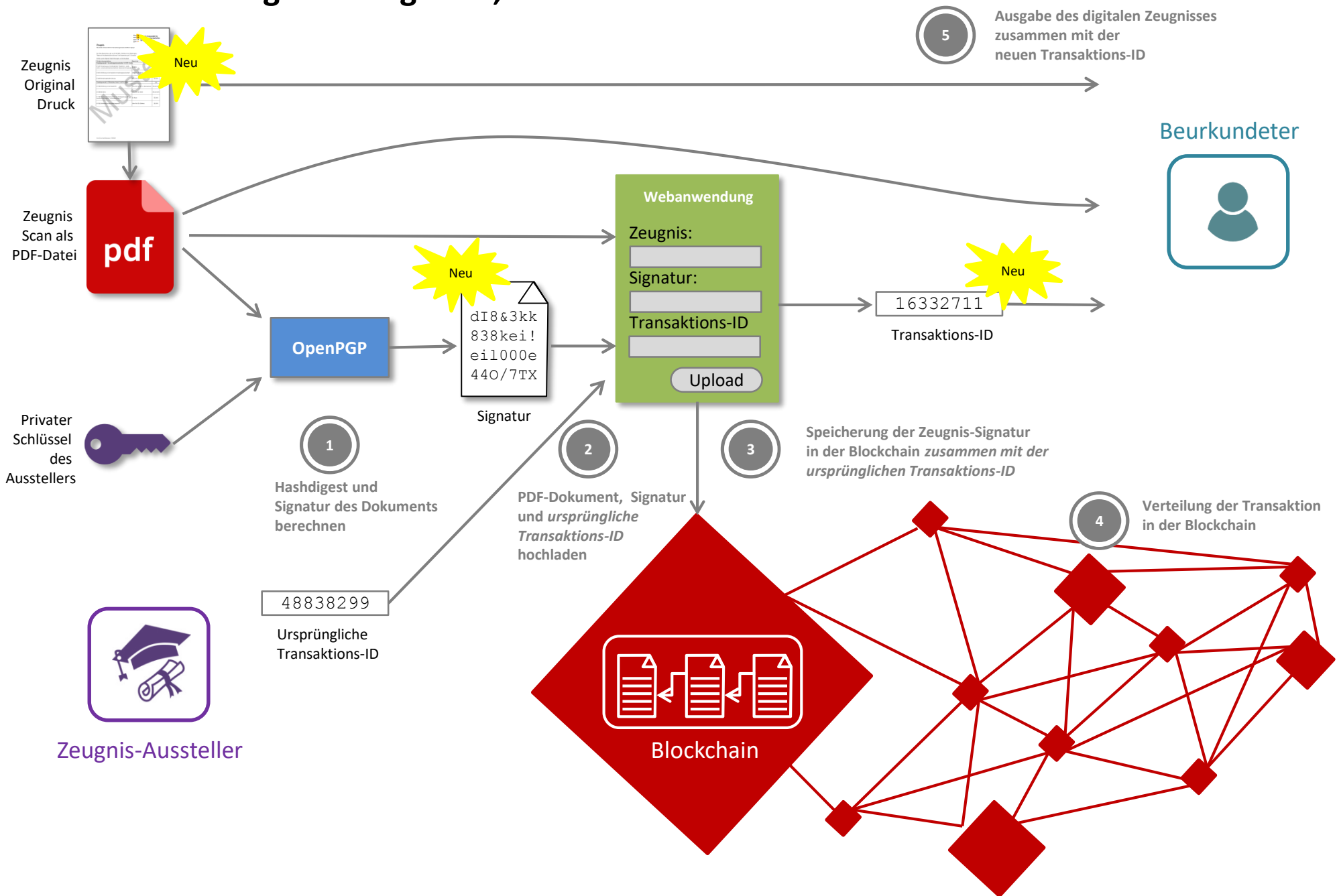
Szenario 1: Zeugnis ausstellen



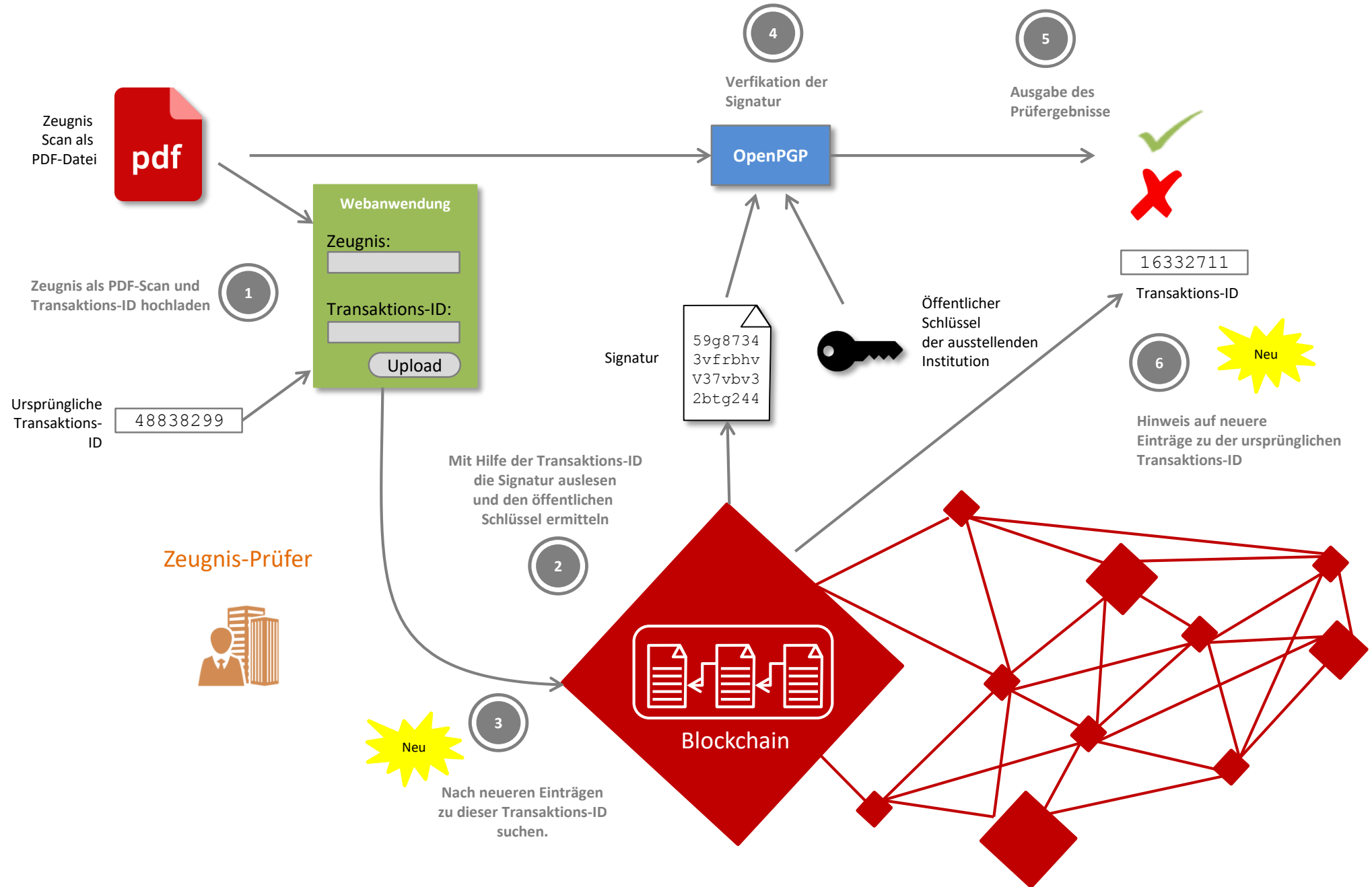
Szenario 2 & 3 : Zeugnisüberprüfung



Szenario 4: Zeugnis korrigieren, aktualisieren



Szenario 2 & 3 : Aktualisiertes Zeugnis überprüfen



Zeugnisvalidierung

Darf jeder Signaturen in der Blockchain speichern?

Nein, unser heutiges Konzept sieht vor, dass nur berechtigte Institutionen in die Blockchain schreiben können. Lesen darf jedoch jeder, die Blockchain ist öffentlich.

Wie funktioniert die Berechtigungsvergabe?

Schreibenden Zugang zur Blockchain bekommen nur Institutionen, deren öffentlicher Schlüssel im System hinterlegt ist. Somit benötigen wir keine Benutzer- und Passwortverwaltung.

Können auch andere Dokumente als PDF verifiziert werden?

Ja, jedes digitale Dokument von dem eine Signatur erstellt werden kann, ist für die Verifikation geeignet.

Ist das System auch für andere Inhalte als Zeugnisse geeignet?

Ja, da prinzipiell jedes digitale Dokument, von dem eine Signatur erstellt werden kann, zur Verifikation geeignet ist, können beliebige Dokumente und Inhalte damit beglaubigt werden.

Wer darf ein Zeugnis überprüfen?

Da jeder die Blockchain lesen kann, kann prinzipiell auch jeder ein Zeugnis überprüfen. Allerdings muss dafür eine Transaktions-ID bekannt sein und für jede Überprüfung fallen Kosten an.

Was passiert, wenn der Beglaubigte seine Transaktions-ID vergisst?

Wenn die Transaktions-ID verloren geht, kann das Zeugnis nicht mehr überprüft werden. Die Daten liegen weiterhin in der Blockchain, sie sind nicht löschbar aber nicht mehr nutzbar, weil sie nicht zugeordnet werden können. Der Beglaubigte kann versuchen die Transaktions-ID beim Aussteller erneut zu erfragen. Wenn dieser sie aber nicht gespeichert hat, muss das Zeugnis in einer neuen Transaktion beglaubigt werden.

Ist es nicht leichtsinnig Zeugnisse öffentlich zugänglich zu speichern?

Es werden keinerlei Inhalte der Zeugnisse in der Blockchain gespeichert sondern nur die zugehörige Signatur. Die Signatur lässt keine Rückschlüsse auf die Zeugnisinhalte zu. Es werden auch keine Namen oder sonstige Merkmale gespeichert, die mit dem Zeugnisinhaber in Verbindung stehen. Die Identifikation eines Eintrags erfolgt ausschließlich anhand der anonymen Transaktions-ID.

Was passiert, wenn der Schlüssel des Ausstellers zurückgezogen wurde?

In diesem Fall kann das Zeugnis offiziell nicht mehr verifiziert werden. Allerdings hält das System eine Kopie des öffentlichen Schlüssels zum Zeitpunkt der Ausstellung vorrätig. In Kombination mit der Blockchain kann also zumindest nachgewiesen werden, das das Zeugnis zum Zeitpunkt der Erstellung gültig gewesen ist. Für eine gültige Verifikation muss der erste Eintrag von der ausstellenden Institution mit dem neuen Schlüssel aktualisiert werden.

Die Zeugnisse ändern sich nur an wenigen Stellen, viele Bereiche in dem Dokument bleiben gleich. Bietet das nicht Angriffsmöglichkeiten !

Es handelt sich um sogenannte "Known Plain Text" Angriffe. Diese sind in diesem Konzept unwahrscheinlich, da wir mit eingescannten Dokumenten, letztendlich also Bildern arbeiten. Durch den Scanvorgang wird jedem Dokument eine gewisse Menge an Zufallszahlen mitgegeben, das sogenannte Seed. Ursache kann z.B. der Scanner sein, der ein gewisses "Rauschen" bei der Erstellung der Bilddatei erzeugt. Zwei unmittelbar hintereinander durchgeführte Einscanvorgänge von demselben Dokument führen somit zu vollkommen unterschiedlichen Signaturen .

Letztendlich muss ich als Überprüfer einer Firma wie der regio iT vertrauen!
Nein, das System ist über die Knoten der Blockchain auf unterschiedliche Firmen verteilt. Die Blockchain ist öffentlich lesbar und damit kann die Integrität der gespeicherten Einträge von jedem zu jeder Zeit überprüft werden. Als Überprüfer kann ich also zu einen Knotenbetreiber meiner Wahl gehen oder die gesamte Blockchain auf meinem lokalen Rechner überprüfen.

Warum ist das sicher?
Wir machen nichts grundsätzlich Neues. In dem Konzept werden lediglich zwei langjährig etablierte Verfahren , die digitale Signatur und die Blockchain, geschickt miteinander kombiniert. Beide Verfahren werden als sicher angesehen, wir möchten an dieser Stelle auf die bestehende Literatur und wissenschaftlichen Untersuchungen verweisen.

Warum wird eine Blockchain verwendet, eine einfache Datenbank würde doch ausreichen?
Einige zentrale Argumente für eine Blockchain finden Sie in Folie Nr. 4. Aus unserer Sicht besonders Vorteilhaft ist der Aspekt der Verteilung, womit eine hohe Verfügbarkeit, Skalierbarkeit und eine langfristige Datenspeicherung im Sinne eines Backups gewährleistet wird. Darüber hinaus ist der in der Blockchain implizit enthaltende Integritätsschutz der Inhalte von zentraler Bedeutung. All diese Aspekte sind in einer Datenbank nicht enthalten und erfordern zusätzliche Maßnahmen .