TeleTrusT
Pioneers in IT security.

TeleTrusT-Informationstag "Elektronische Signatur und Vertrauensdienste" 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 24.09.2019

Trust as a Service

Mirko Mollik, TrustCerts

Verifizierung

- Sicherheit
  - Integritätsüberprüfung
- Elektronische Signaturen
  - Kryptographie
  - Asymmetrische Verfahren
- Relation
  - Öffentlicher Schlüssel und Identität
  - Schlüssel-Management-System

Public Key Infrastructure (PKI)

- Zentrale Dienste
  - Registrierungsstelle
  - Zertifizierungsstelle
  - Sperrliste
  - Verzeichnisdienst
- Hierarchie
  - Kette des Vertrauens

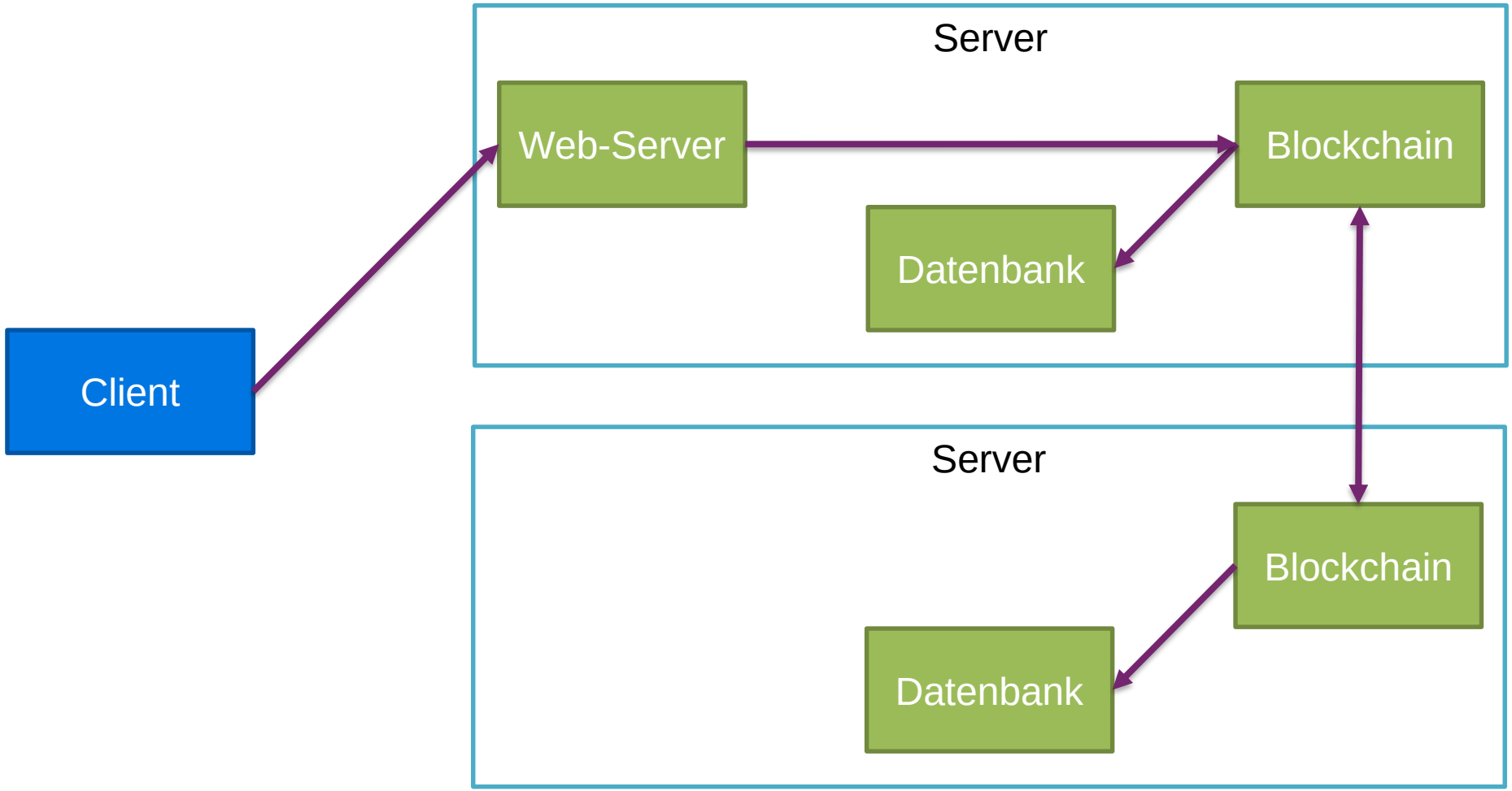
PKI - Sperrregister

- CRL
  - Wird nur 1-2 mal pro Tag aktualisiert
- OCSP
  - „TryLater“ = gültig
  - „Good“ = nicht gesperrt (kann ungültig sein)
  - Als dritte Partei zur Validierung nötig
  - Hohe Auslastung durch individuelle Abfragen

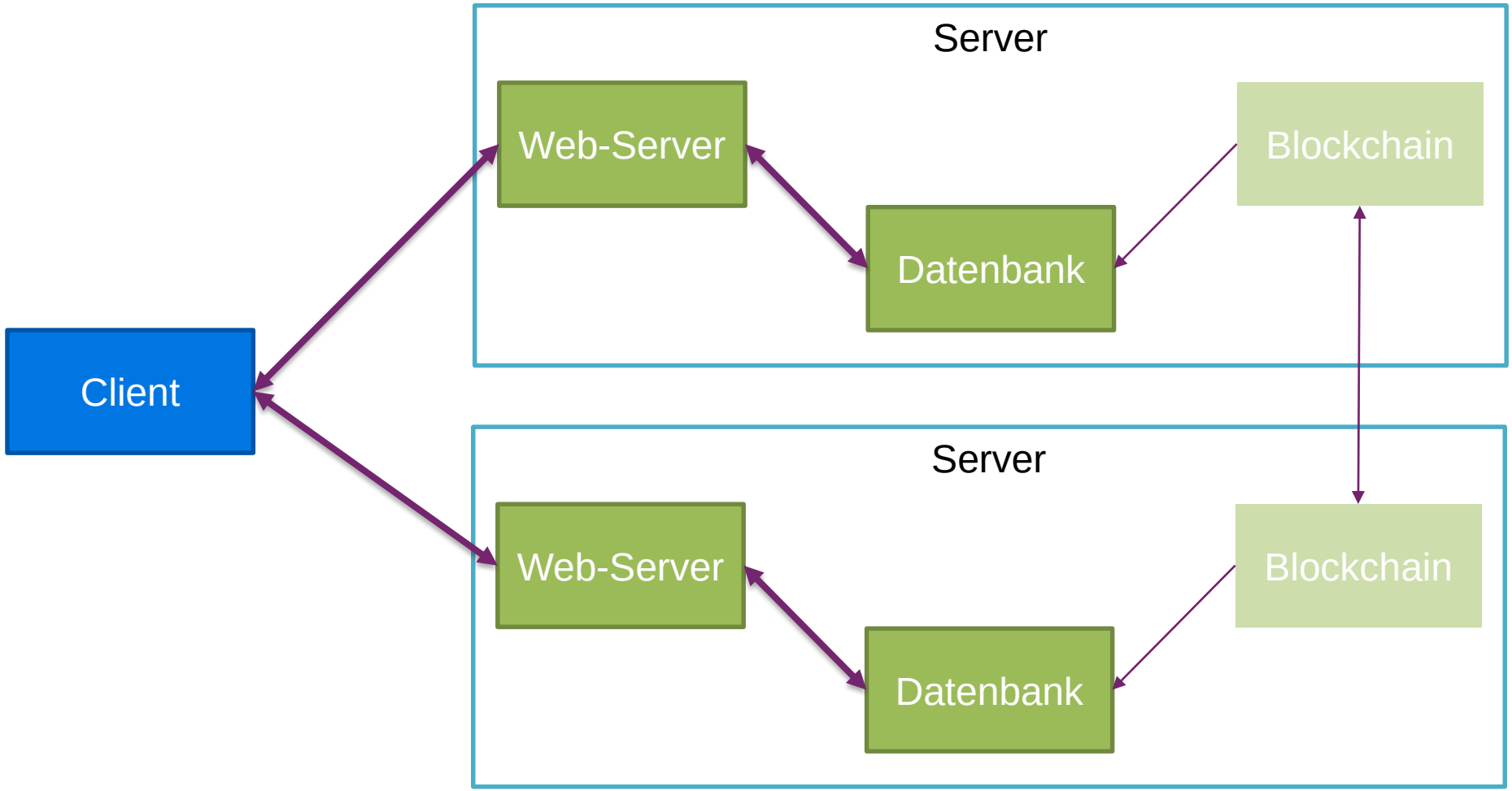
Blockchain

- Verteilt
  - Mehrere Anfragepunkte möglich
- Dezentral
  - Kein Single Point of Control
- Transaktionsspeicher
  - Datenbestand ist synchron
  - Protokollierung der Änderungen
- Konsens
  - Konsistente Zustände

PKI + Blockchain: Eintrag



PKI + Blockchain: Abfrage



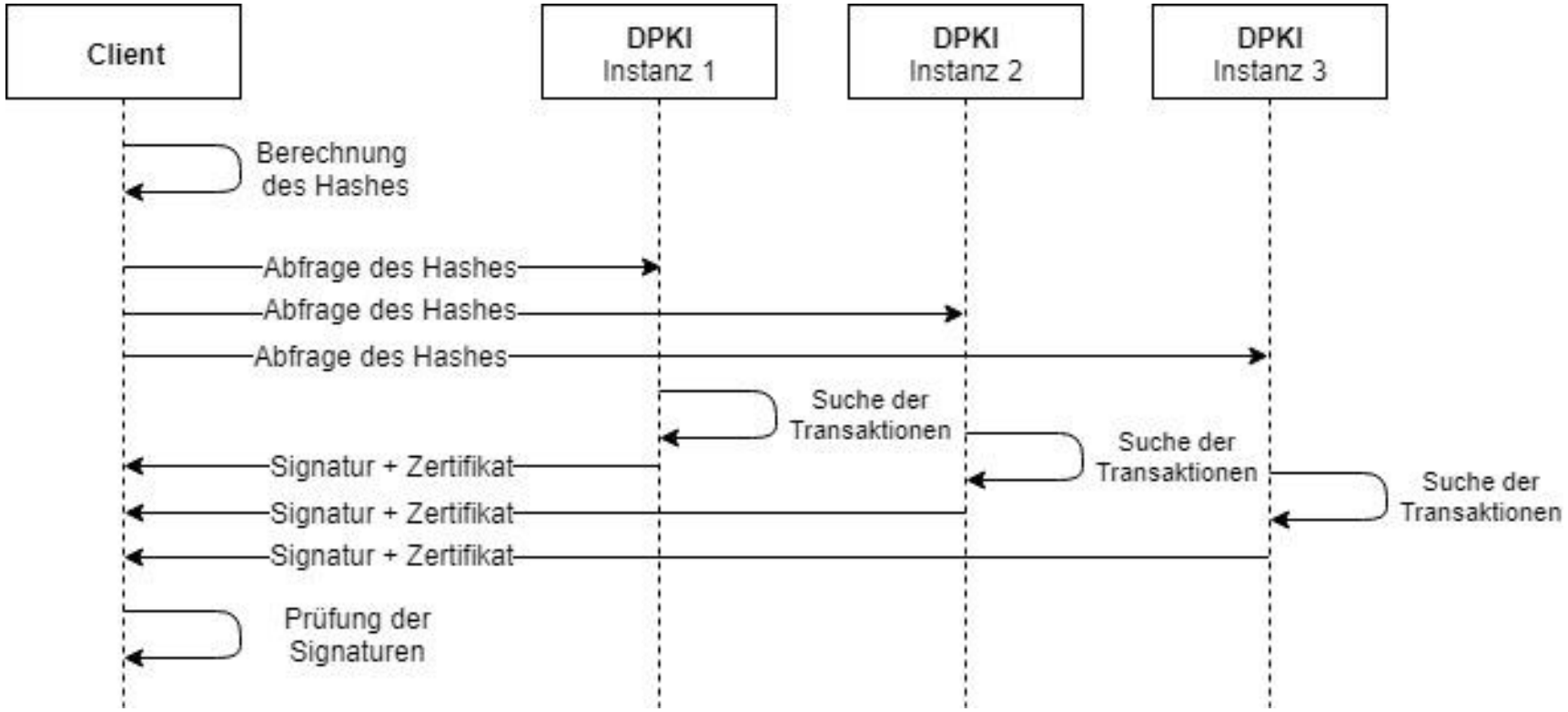
Key Management System

	PKI	DPKI
Vertrauenskette	Muss selber hergeleitet werden	Über Blockchain
Abfrage	Jeder Aussteller aus der Kette	Eine, Abfrage an mehrere Knoten möglich
Single Point of Control	Root-CA	Nein, da Konsortium
Single Point of Failure	Zentrale Zertifizierungsstellen	Nein, jeder Knoten kann genutzt werden
Zertifikat	X509	Dynamisch
Protokollierung	Nein	Durch Transaktionen
Fehlertoleranz	Nein	Über Konsens geregelt

PKI + Blockchain + Signaturspeicher

- Outsourcing der Signatur
  - Unabhängig von Dateityp
  - Protokollierung von Signaturen von Daten
- Datenschutz
  - Speicherung der Prüfsumme: Souveränität bei Weitergabe
  - Identifizierung des Ausstellers

Prozess


Client
DPKI Instanz 1
DPKI Instanz 2
DPKI Instanz 3
Berechnung des Hashes
Abfrage des Hashes
Abfrage des Hashes
Abfrage des Hashes
Suche der Transaktionen
Suche der Transaktionen
Suche der Transaktionen
Signatur + Zertifikat
Signatur + Zertifikat
Signatur + Zertifikat
Prüfung der Signaturen

Vielen Dank für Ihre Aufmerksamkeit