SACHSEN-ANHALT

Landesarchiv

Alles Blockchain oder was? Nutzen und Grenzen der Distributed-Ledger-Technologie in der digitalen Archivierung

Björn Steffenhagen

Landesarchiv Sachsen-Anhalt

13.03.2019

23. Tagung des Arbeitskreises AUdS Prag

Agenda

SACHSEN-ANHALT

Landesarchiv

- Grundlagen
- Aufbau
- Vor- und Nachteile
- Vergleich
- Beispiel Archangel
- persönliche Erfahrungen
- Chancen und Risiken
- Fazit

Grundlagen

SACHSEN-ANHALT

Landesarchiv

- Distributed Ledger = “verteiltes Kassenbuch“
- dezentrales und synchrones Netzwerk bzw. Register mehrerer, gleichberechtigter Teilnehmer (Peer-to-Peer)
- keine zentrale Instanz (Datenbank, Institution) vorhanden

Grundlagen

SACHSEN-ANHALT

Landesarchiv

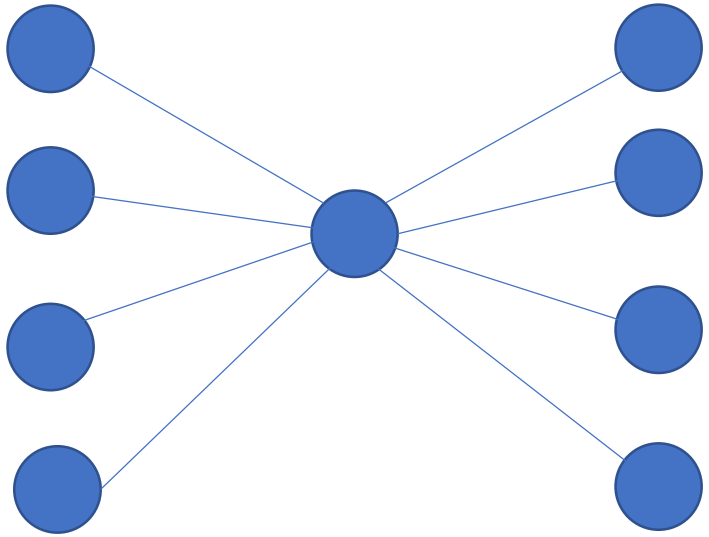
- Validierung mittels Konsensmechanismus
  - Proof-of-Work (PoW): Validierung durch Arbeit
  - Proof-of-Stake (PoS): Validierung durch Besitz
- Vertrauen der Teilnehmer erzeugt durch kryptografische Maßnahmen (Hashfunktionen, Signaturen, PKI)
- Regeln sind in smart contracts (Chaincode) hinterlegt

Architektur: Netzwerk

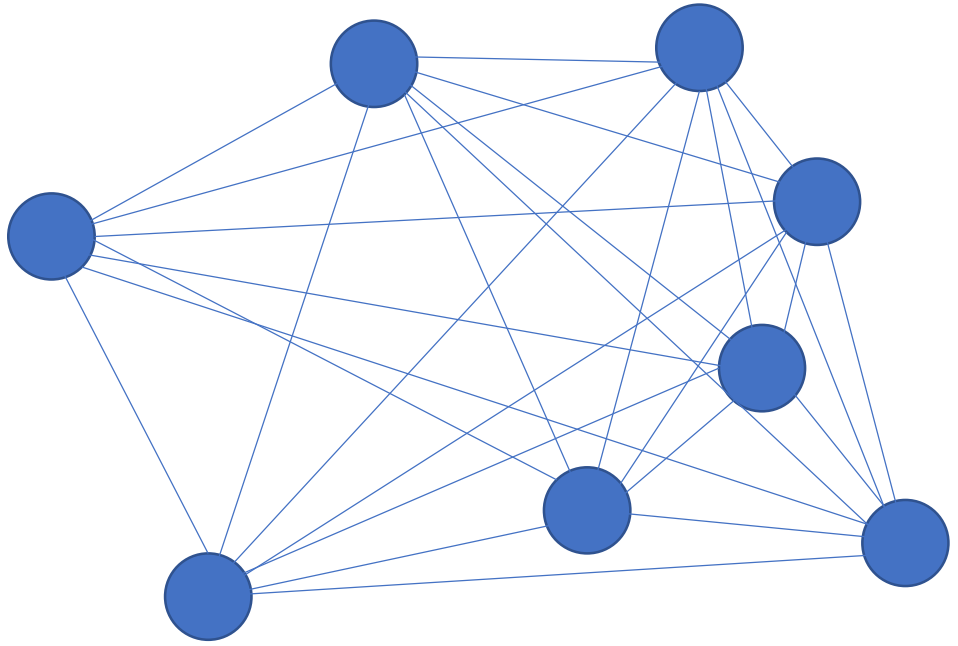
SACHSEN-ANHALT

Landesarchiv

zentrales Netzwerk



verteiltes, dezentrales Netzwerk

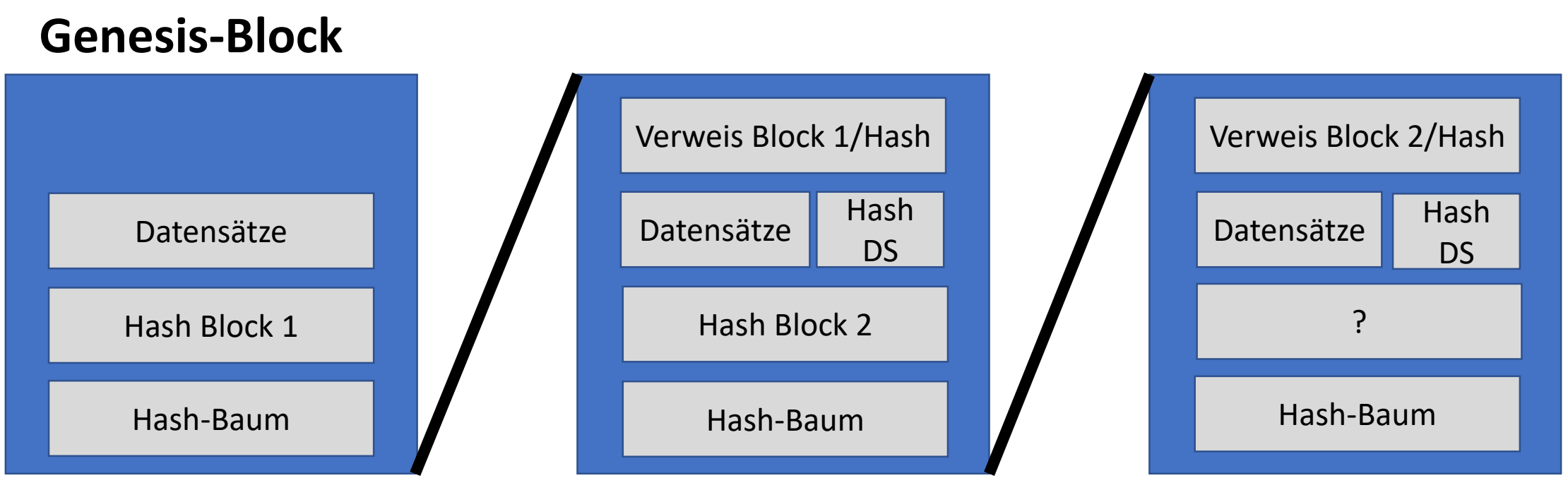


Architektur: Blockchain

SACHSEN-ANHALT

Landesarchiv

stark vereinfacht



Quelle: nach Burgwinkel (2018: Blockchain Technology), S. 6.

Block in der Blockchain – ein Beispiel

Identifier
Difficulty (Schwierigkeitsgrad für den Proof-of-Work)
Nonce (Vorgabe für den Wert des Proof-of-Work)
Hash-Wert aktueller Block
Hash-Wert Vorgängerblock
Zeitstempel
Weitere Signaturen
Hash-Baum (Merkle) der durchgeführten Transaktionen
Transaktionsdaten

Ausprägungen

SACHSEN-ANHALT

Landesarchiv

- Nach Zweck
  - Kryptowährung
  - Transaktionsnachweis
- Nach Zugang
  - public Blockchain: Bitcoin
  - private Blockchain
- Nach Rechten/Besitz
  - Zugriffskontrolle
  - Identitätsnachweis
- Nach Betreiber

Vor- und Nachteile

SACHSEN-ANHALT

Landesarchiv

- Vorteile:
  - Integrität & Authentizität
  - Nachweisbarkeit & Vertraulichkeit
  - dezentrale Strukturen; Intermediäre entfallen

- Nachteile:
  - Overhead & Einsatz von Ressourcen
  - Skalierbarkeit
  - ➢ Wo einsetzen?

Blockchain und Standards

SACHSEN-ANHALT

Landesarchiv

Records Management/Digitale Archivierung

- TR-03138
- eIDAS-VO
- ISO 14721
- DIN 31644/ISO 16363
- TR-03125

- DSGVO
- bisherige Praxis?

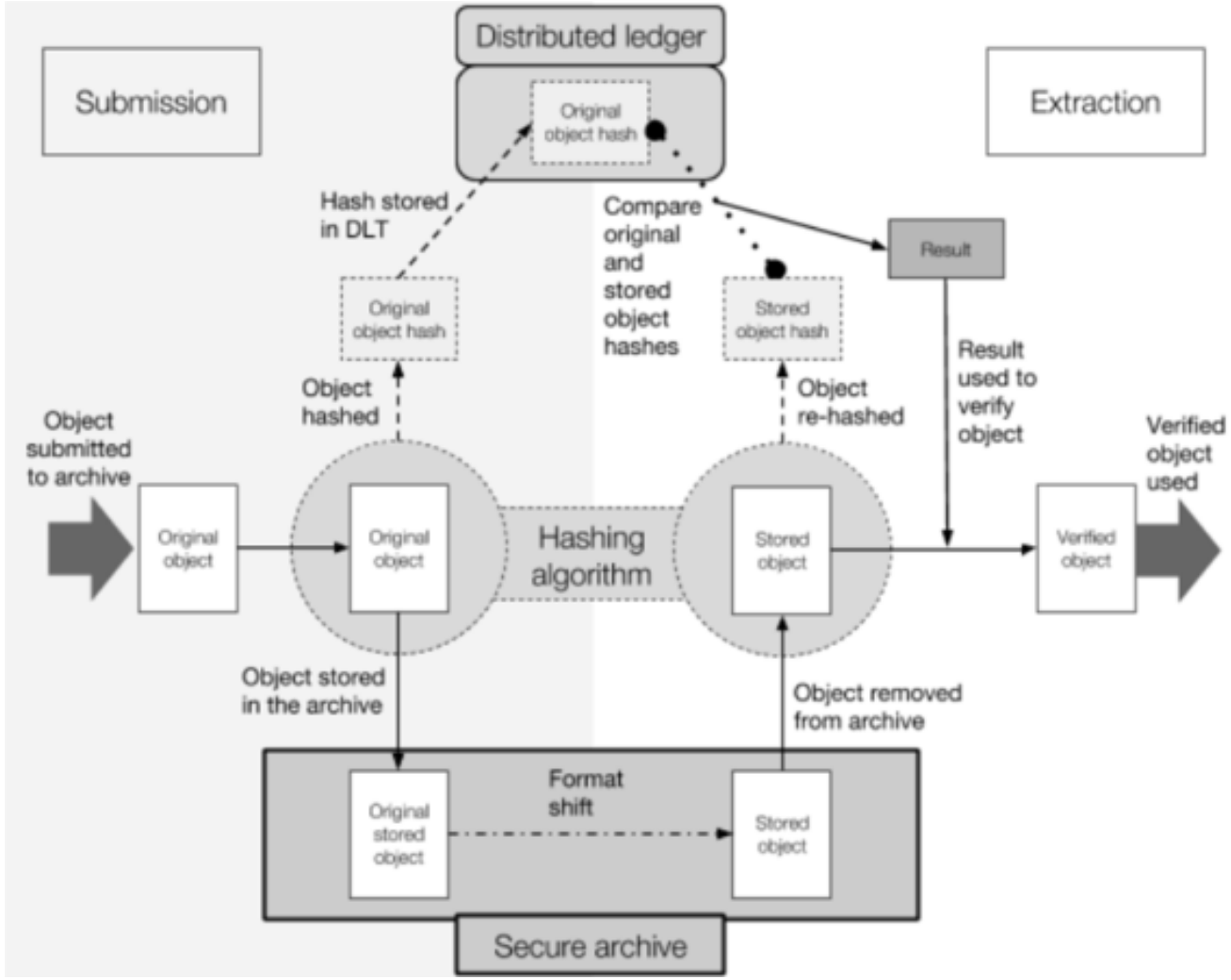
Beispiel: Projekt Archangel

SACHSEN-ANHALT

Landesarchiv

- Förderung ca. 500.000 £
- Zeitraum: 06/2017 bis 06/2019
- Projektpartner: University of Surrey & National Archives UK
- Ziel: Erhaltung von Integrität und authentischen Herkunftsnachweis von digitalen Objekten mittels einer dezentralisierten Blockchain für Gedächtnisinstitutionen
- Umsetzung: Ethereum-Infrastruktur

Architektur Archangel



Quelle: Collomosse, John (2018): ARCHANGEL, S. 2.

Mögliche Architektur einer Blockchain in der dLZA?

- Innerhalb eines Archivverbundes
- Transaktionsdaten statt Primärdaten
- Proof-of-Stake
- Privat und zugangsbeschränkt
- Validierung durch Nutzer muss möglich sein
- Access durch smart contract

Quellen, siehe auch: Schwalm (2019): neue Besen;
Kampffmeyer (2018): Zum Nachdenken;
Kampffmeyer(2019): Konsistentes Löschen.

Risiken

SACHSEN-ANHALT

Landesarchiv

- Schwierige Implementierung bei fachgerechter Umsetzung
- Noch viele Fragen zu klären:
  - Rechtssicherheit?
  - IT-Sicherheit?
  - Standardisierung?

Chancen

SACHSEN-ANHALT

Landesarchiv

- Erhaltung von Integrität, Authentizität und Nachweisbarkeit

-> Ius Archivi?

- Anpassbar auf persönliche Bedürfnisse
- Viele Akteure beschäftigen sich mit der Thematik
- Es gibt erste Vorbilder

Fazit

SACHSEN-ANHALT

Landesarchiv

- Es gibt viele Herausforderungen, Blockchain löst sie nicht (alle)
- Datenschutz größte Herausforderung
- Stand der Technik
- Blockchain ist ein interessanter Ansatz für die digitale Archivierung!
- Was brauchen/wollen wir eigentlich?

Quellen

SACHSEN-ANHALT

Landesarchiv

Antonopoulus, Andreas (2018): Bitcoin und Blockchain – Grundlagen und Programmierung, 2. Aufl. Heidelberg.

Burgwinkel, Daniel (Hrsg.) (2016): Blockchain Technology, Berlin, Boston.

Collomosse, John (2018): ARCHANGEL: Trusted Archives of Digital Public Documents, in: ACM Document Engineering 2018 UF https://arxiv.org/abs/1804.08342 [13.03.2019].

Ebersbach, Jan (2018): Blockchain-Anwendungen. Blockchain im praktischen Einsatz, in: iX. Magazin für professionelle Informationstechnik, Nr. 7, S. 50-54.

Green, Alex et. al. (2018): Using Blockchain to Engender Trust in Public Digital Archives, in: iPRES 2018 15th International Conference on Digital Preservation, Sep 2018, Boston, USA, URL: https://mfr.osf.io/render?url=https://osf.io/rbyzu/?action=download%26mode=render [13.03.2019].

Kampffmeyer, Ulrich (2018): Zum Nachdenken auf dem Nachhauseweg – The Future of Finance Applications & Information Management, Vortrag auf der EuroFaktura 2018, Vortragsfolien. URL: https://www.slideshare.net/DRUKFF/de-zum-nachdenken-auf-dem-nachhauseweg-the-future-of-finance-applications-information-management-dr-ulrich-kampffmeyer-eurofaktura-2018-hamburg [13.03.2019].

Kampffmeyer, Ulrich (2019): Konsistentes Löschen in der Block Chain. URL: https://project-consult.theum.com/newsletter/index.htm?t=Kunden-Newsletters-ab-2011,2019,201901-Februar,Artikel,Konsistentes-L%C3%B6schen-in-der-Block-Chain [13.03.2019].

Keitel, Christian; Schoger, Astrid (Hrsg.) (2013): Vertrauenswürdige digitale Langzeitarchivierung nach DIN 31644, Berlin, Wien, Zürich.

Lemieux, Victoria (2016):Trusting records: is Blockchain technology the answer? Records Management Journal 26, Nr. 2, S. 110-139. URL: https://doi.org/10.1108/RMJ-12-2015-0042 [13.03.2019].

National Archives and Records Administration (2019): Blockchain White Paper. URL: https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf [13.03.2019].

Schrimpf, Sabine (2014): Das OAIS-Modell für die Langzeitarchivierung. Anwendung der ISO 14721 in Bibliotheken und Archiven, Berlin, Wien, Zürich.

Schwalm, Steffen (2019): Neue Besen im Spannungsfeld eIDAS und DSGVO-Blockchain für (dauerhafte) Verzeichnisdienste? Folien CAST-Workshop „PKI - Elektronische Vertrauensdienste“, DOI:10.13140/RG.2.2.17838.36163.

Seeger, Jürgen (2018): Von Bitcoin bis Ripple. Hyperledger-Implementierungen im Vergleich, in: iX. Magazin für professionelle Informationstechnik, Nr. 7, S. 44-48.