



iSAQB goes Blockchain?

consensus in decentralized applications

Lars Hupel und Marcus Klüsener

INNOQ / ITech Progress

Blockchain? Was ist das eigentlich?

Mittwoch, 16.10.2019 | 11:00 - 11:45 Uhr |  Mi 1.1

Distributed Ledgers, Blockchains und andere seltsame Dinge



Stefan Tilkov

INNOQ

Geschäftsführer und Principal Consultant

In diesem Vortrag werden wir uns mit einem der am meisten „gehypten“ Technologiethemen der letzten Jahre auseinandersetzen: der Blockchain, technologische Basis für Kryptowährungen wie Bitcoin und Plattformen wie Ethereum, und der daraus abgeleiteten Verallgemeinerung Distributed Ledger Technology (DLT). Nach der kürzesten Einführung der Welt werden wir uns vor allem mit den drei wichtigsten Fragen, die sich für Architektinnen und Architekten stellen: Was genau ist denn nun das Neue daran, und welche Eigenschaften ergeben sich daraus? Welche Ausprägungen gibt es und worin unterscheiden sie sich? Und vor allem: Wann ist eine Blockchain/DLT-Lösung sinnvoll und wann ist sie abwegiger Unsinn?

Nochmal von vorne ...

- 2009: Bitcoin
- 2015: Ethereum
- 2019: iSAQB-Modul *Blockchain*

Alter Wein in neuen Schläuchen?

MOTHERBOARD
TECH BY VICE

The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995

This really gives a new meaning to the "paper of record."

By [Daniel Oberhaus](#)

Aug 27 2018, 10:19pm [Share](#) [Tweet](#)

**NOTICES &
LOST AND
FOUND**
(5100-5102)

Universal Registry Entries:
Zone 2 -
dS8492cgVOFAoP9kyE1XzMOrQ
HgEwzkVbVafNvIkUz99qvq8/ME
p5y9EFSG8XxzMBalGQQ==
Zone 3 -
JnFCg+HCmvhj8GmmUP7VZna71
NgZup/RfuKUQNzCHWXMuaLK
durxHQV5pSHLaBGPRly+mg==
These base64-encoded values represent the combined fingerprints of all digital records notarized by Surety between 2009-06-03Z 2009-06-09Z.
www.surety.com 571-748-5800

Quellen:

https://www.vice.com/en_us/article/j5nzx4/what-was-the-first-blockchain

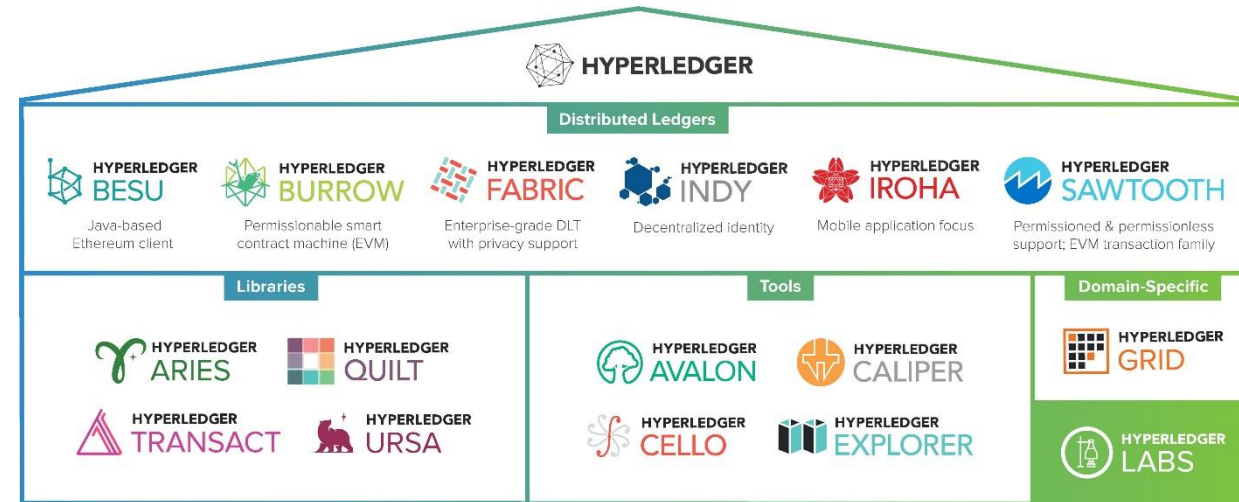
<http://surety.com/digital-copyright-protection/prove-ownership>

Zeit für Software-Architektur

- Blockchain ist absolutes Hype-Thema
- alle wollen irgendwie mitspielen, aber keiner weiß wie es genau funktioniert
- Thema kommt langsam im Enterprise-Umfeld an

Blockchain ist wilder Westen

- keine Standards
- keine einheitliche Terminologie
- viele (zweifelhafte) Startups
- Goldrausch-Mentalität



Unser Beitrag

iSAQB-Lehrplan *Blockchain*:

- Veröffentlichung dieses Jahr
- unaufgeregt & ausgeglichen
- wichtigste Kenntnisse für Architekt*innen und Entscheider*innen
- kooperativ entwickelt

Kapitel 1: Grundlagen

- Definitionen, Begriffsklärung
- kryptografische Grundlagen
- Konsensverfahren
- Trade-offs

Kapitel 2: Smart Contracts

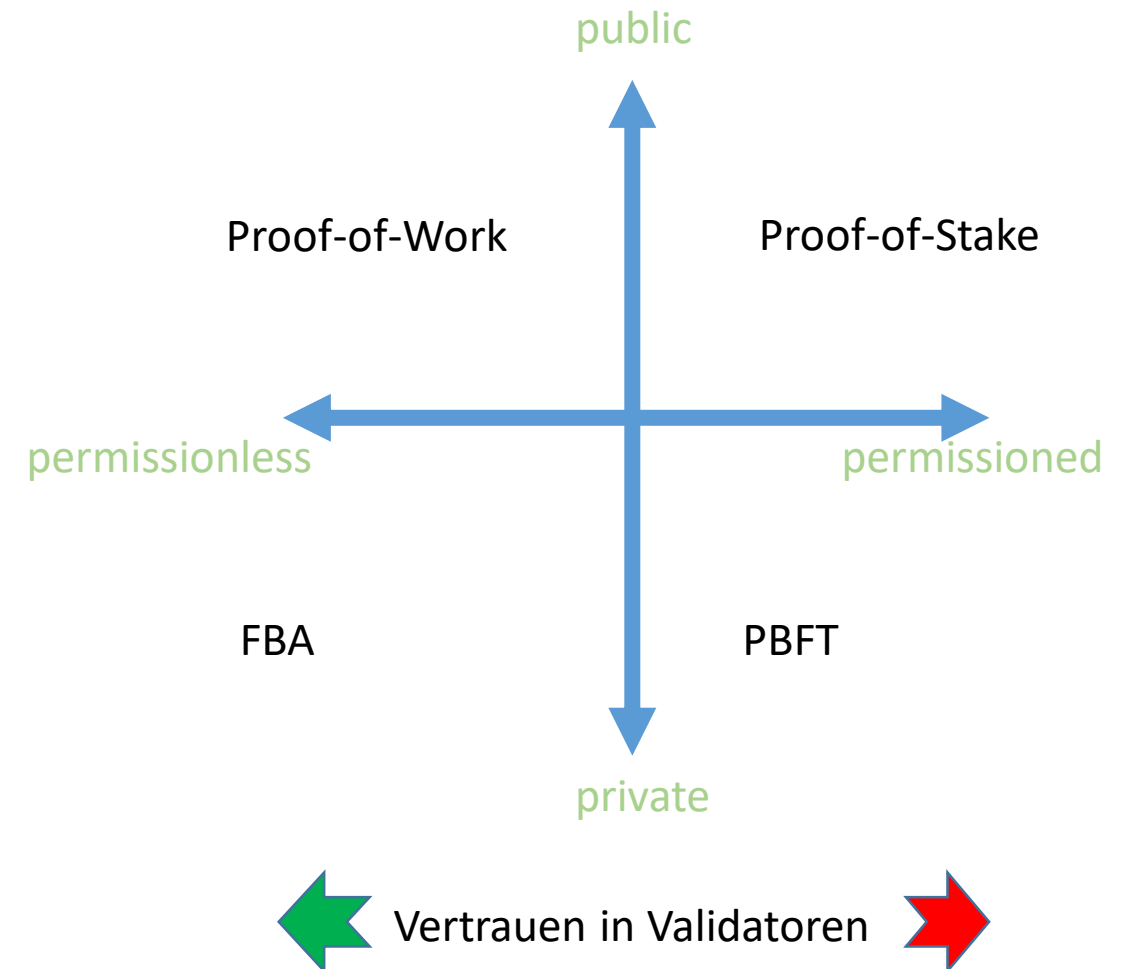
- Verwendungszweck
- Entwicklungsmethoden
- virtuelle Maschinen
- Sicherheitsrisiken

Kapitel 3: Flavours & Use Cases

- Proof-of-Work, Proof-of-Stake, Proof-of-Authority
- Zugriffskontrolle & alternative Konsensverfahren
- Sprachen für Smart Contracts
- Entscheidungskriterien Anwendungsfall $\leftrightarrow$ Technologie

Kapitel 4: Permissioned Blockchain

- Implementierungen mit mehr Freiheitsgraden und Flexibilität
- Lösung, um interne Prozesse nicht in einer Public Blockchain zu veröffentlichen
- Überblick über die wichtigsten Merkmale (Kosten, Performance, Governance)

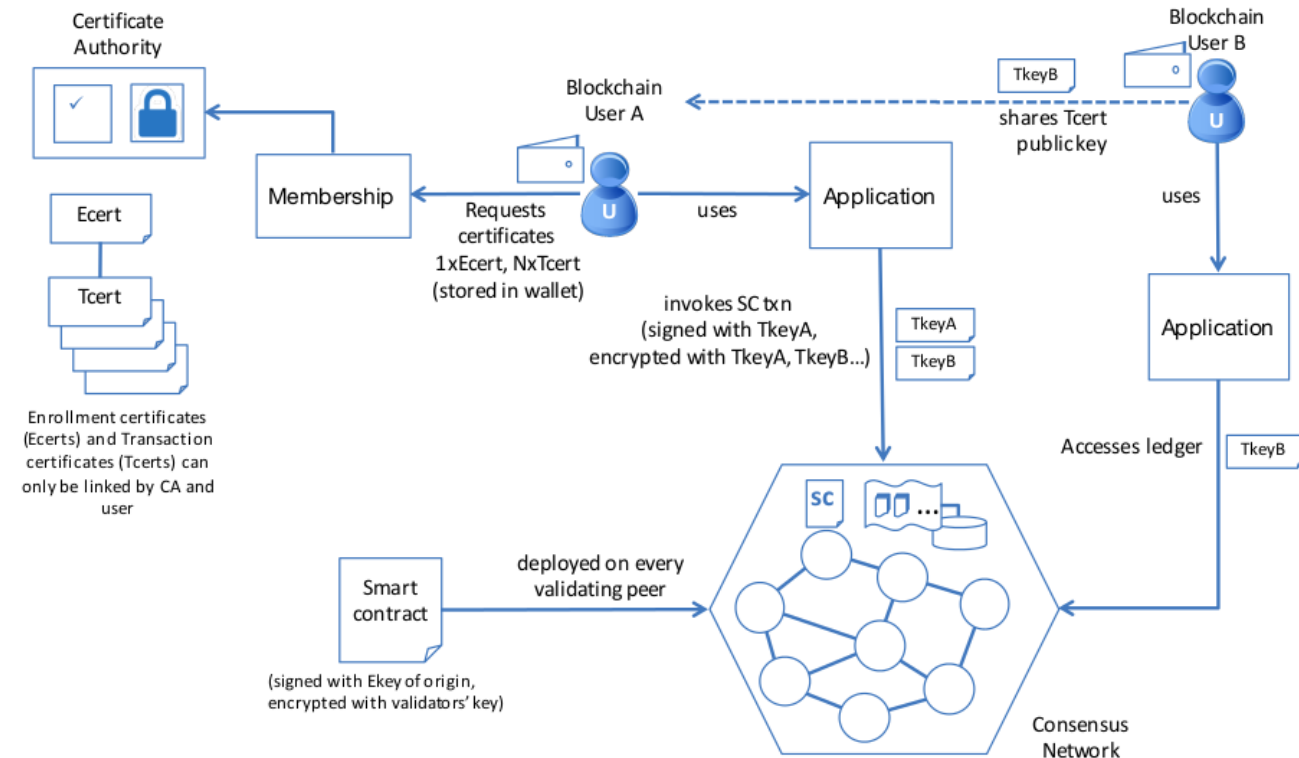


Kapitel 4.1: Permissioned Blockchain

- Anwendungsfälle bei denen permissioned Blockchains Vorteile bieten
- Vorteile einer expliziten Governance
 - Unterschiede zwischen In-Chain- und Off-Chain-Governance
 - Zugriff, Nutzerrechte, Verifikation und Netzwerkstruktur an die Governance-Anforderungen anpassen
- Nachteile der Wiedereinführung eines bestimmten Zentralisierungsgrades
- Analyse der Qualitätsattribute von permissioned Blockchains (z. B. Corda, Hyperledger, Enterprise Ethereum)
- Auswirkungen verschiedener Konsensus-Algorithmen
- Technologischen Unterschiede bei der Implementierung

Kapitel 4.2: Infrastruktur

- Benötigte Infrastruktur für Permissioned Blockchains
- Standards zur Authentifizierung und Verschlüsselung (X.509 und TLS)
- Deployment Patterns
- Sicherheit für permissioned Blockchains

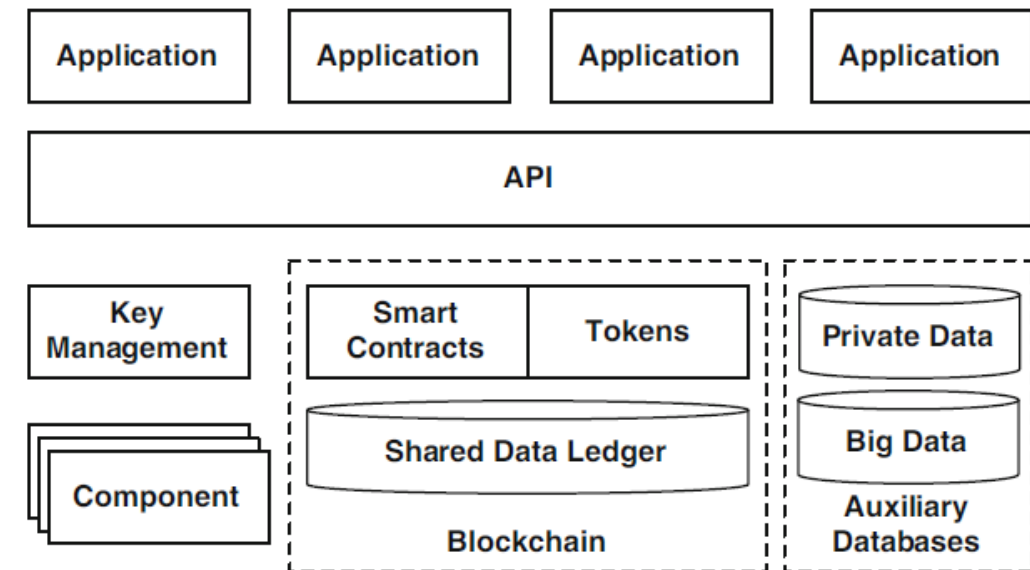


Infrastruktur einer Permissioned Blockchain

Quelle: <https://mastanbtc.github.io/blockchainnotes/blockchaintypes/>

Kapitel 5: Architecture

- Smart Contracts allein reichen nicht aus, um Blockchain-basierte Anwendungen zu erstellen.
- Sie benötigen eine externe Infrastruktur, die die Interaktionen zwischen Benutzern und Verträgen ermöglicht.
- Dezentralisierung ist das Schlüsselmuster für den Entwurf robuster Anwendungen.



Blockchain in a software architecture. Quelle: Xu et al.

Kapitel 5.1: Architecture

- Blockchain als Softwarekomponente für Speicherung, Berechnung und Kommunikation
- Prozesse zum Entwerfen von Blockchain-Anwendungen
- Muster für Interaktion, Datenmanagement, Sicherheit und Vertragsstruktur (z.B. Oracle, On-Chain Data, Tokenization)
- Integration in ein Enterprise System
- Prinzipien einer dezentralen Anwendung (DApp)
 - Smart Contract und Webanwendung

Kapitel 5.2–5.4

- Skalierbarkeit
 - Wie skalieren public und private Blockchain-Implementierungen
 - Abschätzung von benötigter Rechenleistung
- Speicherbedarf
 - Speicherformat und Kapazität auf Blockchains
 - On- und Off-Chain Storage
- Datenschutz und Governance
 - Unveränderlichkeit von Transaktionen in der Blockchain (DSGVO)
 - Zero-Knowledge Proofs





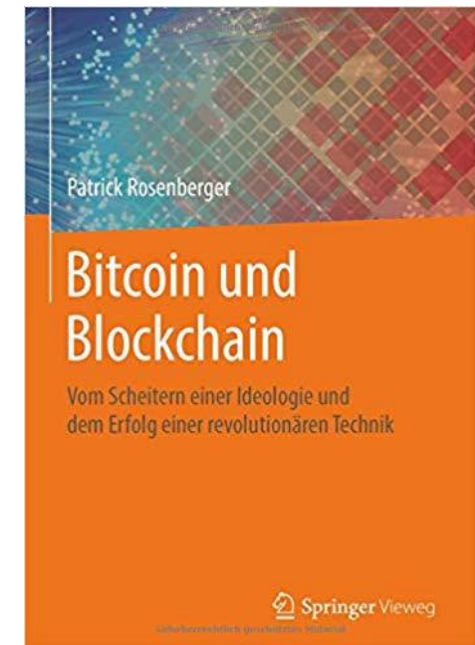
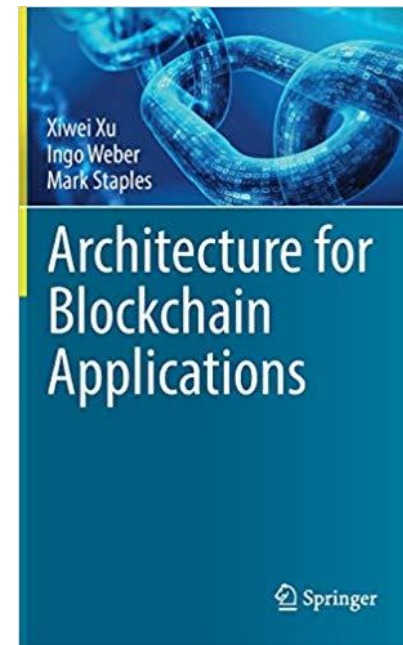
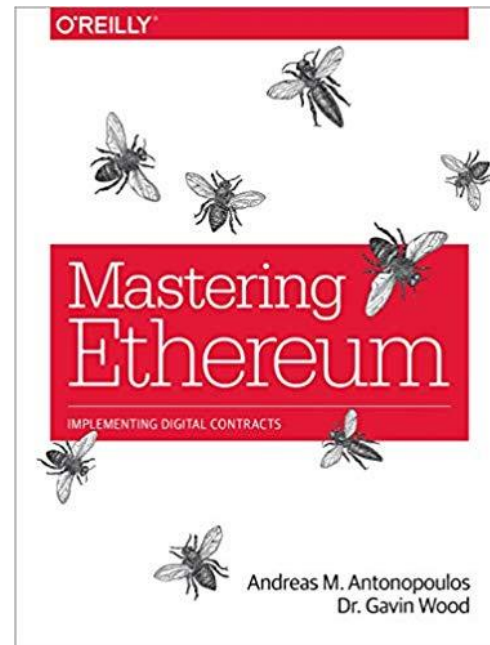
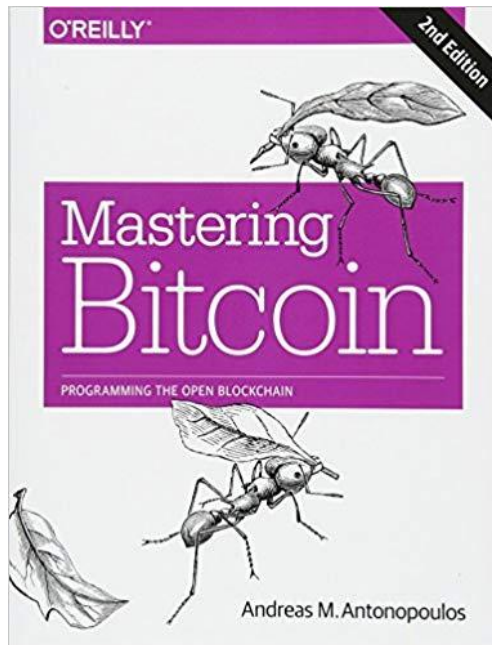
iSAQB-geschulter Software-Architekt

- Foundation Level: eine dem Problem angemessene Software-Architektur entwerfen
- AWERT (Architektur-Bewertung): wie findet man heraus, ob eine Architektur die Erwartungen erfüllt
- IMPROVE (Evolution und Verbesserung): wie verbessert man Softwaresysteme systematisch, ausgerichtet an ökonomischen und technischen Zielen
- WEB (Web-Architekturen): wie gestaltet man leistungsfähige und sichere webbasierte Systeme
- BLOCKCHAIN (Low-Trust Consensus in Decentralized Applications): wie konzipiert und implementiert man konsensbasierte dezentrale Anwendungen



Q & A

Literatur



... und viele weitere

Diskussionspunkte

1. Titel Blockchain oder weiter fassen?
2. Welchen Stellenwert sollen Praxisbeispiele haben?
3. Wie genau sollen wir auf die Probleme, die man mit einer Blockchain-Architektur lösen kann, eingehen?
4. Was löst das Buzzword „Blockchain“ aus und wie viel (oder wie wenig) hat das mit dem Lehrplan zu tun?
5. architecting / engineering / designing