Bewertungs- und Entscheidungshilfe bei der Auswahl der passenden Blockchain-Technologie

K. Wittek[1], T. Spielmann[1]
[1] Institut für Internet-Sicherheit – if(is), Westfälische Hochschule, Gelsenkirchen, Deutschland
kontakt_reallabor@fit.fraunhofer.de

Ausgangssituation und Problemstellung

Die auf einer Blockchain-Node laufende Software zur Verwaltung bzw. Vorhaltung der Daten ist eine der Kernkomponenten eines Blockchain-Systems (gem. [2] Kap 1.1 S.10). Daher ist dieser Bereich sehr kritisch und schützenswert. Neben den Schutzmechanismen in den Komponenten um den Kern, sollte auch der Kern selbst nach bestem Wissen und Gewissen abgesichert werden. Jedoch dürfen unter diesen Maßnahmen weder die Funktionalität noch die Performance über Gebühr beeinträchtigt werden.

Anwendungskontext

Die Beantwortung dieser Forschungsfrage soll dazu dienen, verschiedene Blockchain-Implementierung gegeneinander abwägen zu können. Hierbei kann allerdings keine pauschale Bewertung vorgenommen werden. Es muss immer der jeweilige Kontext und die Umgebung berücksichtigt werden, in der die Blockchain eingesetzt werden soll. Hierbei gilt es zunächst eine geeignete Struktur in Hinblick auf Zugriffs- und Validierungsrechte zu finden.

Zugriffsrechte: public oder private Blockchain

Eine public Blockchain bedarf keines großen organisatorischen Aufwandes. Dafür muss hier ein großes Augenmerk auf die Vertraulichkeit und Integrität der Daten gelegt werden. Da es keine Zugriffsrechte gibt, muss sichergestellt werden, dass nicht-öffentliche Daten geschützt werden. Anders verhält es sich bei private Blockchains. Hier existieren Zugriffsrechte. Diese müssen verwaltet werden, was für einen erhöhten organisatorischen Aufwand sorgt. Daher wird es ein Punkt dieser Forschungsfrage sein, den organisatorischen Aufwand gegen die notwendigen Sicherheitsanforderungen abzuwägen.

Validierungsrechte: permissionless oder permissioned Blockchain

Analog dazu verhält es sich mit den Validierungsberechtigungen in einem Blockchain-System. Eine permissionless-Blockchain ist analog zur public-Blockchain mit weniger organisatorischem Aufwand verbunden. Da hier jeder Teilnehmer Blöcke validieren/signieren und somit der Blockchain hinzufügen darf, ist die Existenz eines Rechtesystems nicht notwendig. Um dennoch die fehlerhafte oder sogar böswillige Erzeugung von falschen Blöcken zu verhindern, ist ein starker Konsensmechanismus notwendig, da jeder Teilnehmer potentiell nicht-vertrauenswürdig ist. Anders sieht es bei einer permissoned-Blockchain aus. Hier sorgt das Identitäts- und Rechtemanagement für mehr Vertrauenswürdigkeit, macht aber den sicheren Umgang von Schlüsselmaterial umso wichtiger. Daraus folgt ein weiterer Punkt der Forschungsfrage: Wie ist das Verhältnis zwischen Mehraufwand und Mehrnutzen durch das (nicht-)Vorhandensein eines Rechtesystems und für welche Fälle ist welche Variante angemessen?

Nach der Unterscheidung und Risikobewertung der grundlegend Strukturmöglichkeiten einer Blockchain ist es ebenfalls notwendig, die auftretenden Bedrohungen in ein Thread Model für Blockchain-System einzuordnen:

Neu aufgetretene, blockchainspezifische Bedrohungen

Das Konzept der Blockchain und ihrer Anwendungsfälle ist noch genau so neu wie unbekannt. Neben den vielen neuen Möglichkeiten entstehen ebenso neuartige Bedrohungen, welche für die bisher bekannten Konzepte noch weitgehend unbekannt bzw. unbedeutend waren. Diese gilt es insbesondere zu erforschen. Ein umfangreiches Wissen, sowie ein guter und umsichtiger Umgang mit diesen neuen Bedrohungen ist daher unumgänglich. Da es in dieser

Forschungsfrage vornehmlich um den Blockchain-Kern gehen soll, ist diese Kategorie besonders wichtig und umfangreich zu bearbeiten.

Beispiele:

- 51% - Angriff
- Sicherheit der Konsenzmechanismen (z.B. provozieren von Timeouts)
- Selfish-Mining
- Sorgfalt und Fehlerfreiheit der Programmierungen

Bereits bekannt Bedrohungen, welche im Kontext Blockchain neu bewertet werden müssen

Ein Blockchain ist ein verteiltes, aber auch komplexes Informationstechnisches System, bestehend aus einem zumindest teilvermaschten Computernetzwerk. Diese Netzwerktopologie, sowie auch der generelle Betrieb eines Knotens in einem Netzwerk sind altbekannte Konzepte der Informatik. Somit sind auch die Probleme dahinter weitgehend bekannt und lösbar. Doch die Tatsache, dass auf diesen Knoten ein Blockchain-System läuft, macht eine Neubewertung der bereits bekannten Probleme notwendig.

Beispiele:

- Sicherheit der genutzten kryptografischen Verfahren
- Sicherheit / Kollisionsresistenz der genutzten Hashfunktion(en)
- (D)DoS-Angriffe
- Eclipse-Angriffe

Systemunabhängige Bedrohungen und deren Behandlung

Wie bereits festgestellt ist eine Blockchain auch ein informationstechnisches System. Jedes IT-System hat eine gewisse Art und Anzahl von Bedrohungen, abhängig von Topologie, Anwendungsfällen oder Größe. Sobald mindestens eine Komponente des Systems ein Teil eines Netzwerks und/oder über das Internet zugänglich ist, muss eine Reihe von "Standard-Bedrohungen" ebenfalls beachtet werden.

Beispiele:

- Penetrationtesting
- Backup and Recovery
- Identitymanagement

Lösungsansätze

Die zuvor genannte Einteilung erhebt selbstverständlich keinen Anspruch auf Vollständigkeit. Hiermit soll lediglich eine grobe Struktur aufgezeigt werden. Sicherlich ist eine Ergänzung, sowie feinere Unterteilung notwendig und sinnvoll.

Für einige der genannten Bedrohungen gibt es bereits fertige Lösung oder zumindest Lösungsansätze. Diese können im Rahmen dieser Forschungsfrage aufgegriffen, weiterverfolgt, bewertet und konkurrierende Lösungen gegeneinander abgewogen werden.

Als Ergebnis dieser Forschungsfrage wäre ein Leitfaden denkbar. Dieser kann als Entscheidungshilfe und zur Gewichtung von Blockchain-Implementierung dienen. Jedoch kann eine Implementierung niemals pauschal bewertet werden.

Literatur

1. Arunkumar, S. & Muppidi, S., 2019. Secure your blockchain solutions. [Online]
2. Available at: https://developer.ibm.com/technologies/blockchain/articles/how-to-secure-blockchain-solutions/.
3. Bundesamt für Sicherheit in der Informationstechnik (BSI), 03/2019 "Blockchain sicher gestalten - Konzepte, Anforderungen, Bewertungen", https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=5
4. Ittay Eyal, Emin Gün Sirer, 11/2013, "Majority is not Enough: Bitcoin Mining is Vulnerable", https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf
5. Norbert Pohlmann, 2019, "Cyber-Sicherheit - Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung", Kapitel 14.6 Sicherheit und Vertrauenswürdigkeit der Blockchain-Technologie

Forschungseinrichtungen

Zur Bearbeitung dieser Forschungsfrage sind Kompetenzen aus folgenden Bereichen erforderlich:

- Mathematik (Kryptographie)
- Informatik (Cyber-Security, Verteilte Systeme, Netzwerke)