Fragen und Antworten zu Geschäftsmodellen mit Blockchain

FAQ Sammlung zum Webinar "Neue Geschäftsmodelle mit Blockchain" vom 6.12.2018

Technik

1. Was ist der Unterschied zwischen digitalem Fingerabdruck und digitaler Signatur?

2. Warum haben Sie genau das Modell von Wüst et al. verwendet? Es gibt mittlerweile schon einige "Entscheidungsbäume" die alle Ihre Vor und Nachteile haben.

3. Gibt es schon Überlegungen die Software-Qualität der unterschiedlichen Blockchain-Technologien bzw. -Module sicherzustellen bzw. zu standardisieren?

4. Was sind NODES? Wie funktionieren diese?

5. Wie verhält es sich mit den immer wieder angesprochenen hohen Energieverbräuchen bei Blockchain-Anwendungen?

Sicherheit und Rechtliches

6. Wie gehe ich mit persönlichen Daten auf der Blockchain um (hinsichtlich DSGVO)?

7. Wie beurteilen Sie die Blockchain im Licht der EU-DSGVO (Unveränderbarkeit der Blockchain vs. 'Recht auf Vergessen werden' in der DSGVO)?

8. Wenn ich Daten auf der Blockchain freigebe, wäre es ja für den Leser möglich, diese Informationen zu kopieren und für sich zu nutzen. Ist das möglich?

9. Zum Beispiel Diebstahl: Wie wird verifiziert, dass der Diebstahl "echt" war? Risiko missbräuchliche Schädigung in Chains?

10. Wie wird bei Everledger das Zertifikat beim Kauf an den Kunden übergeben? Und was würde im Fall des Verlusts dieses Zertifikats passieren? Eine Identifikation ist in diesem Fall nicht mehr möglich und somit kann ein eventueller Diebstahl nicht validiert werden.

Blockchain-Anwendungen

11. Werden sich die "Währungen" wie BTC durchsetzen oder werden sie verschwinden?

12. Macht Mining noch Sinn oder gibt es für die Zukunft Alternativen?

13. Kann die Kryptowährung bzw. Blockchain die nächste "Tulpenkrise" hervorrufen?

14. Wo kann ein Unternehmer in der Praxis konkret die Blockchain anwenden? Sind das gewisse Software-Programme?

15. Was an der Blockchain Technologie ist speziell für KMU von Bedeutung/von Nutzen?

16. Welche Innovationen sind insgesamt mit dieser Technologie denkbar (abgesehen von Kryptowährungen)?

17. Ist die Blockchain auch dafür geeignet, eine Cloud zu ersetzen, wo z.B. Kunden sensible Daten ablegen könnten?

18. Sind bereits touristische Anwendungen bekannt abseits der Flugverspätungs-Auszahlung?

19. Welche Anwendungsbeispiele fallen Ihnen für die Baubranche ein? Gibt es schon welche, international?

20. Wo sind die größten Hürden beim Einstieg in die Blockchaintechnologie?

21. Ist der Einstieg in Blockchain eine Angelegenheit, die von den IT-Experten eines Unternehmens allein getroffen werden kann, oder ist dies eher

"Chefsache" (Steuerung durch Geschäftsleitung)?

22. Wie können CIOs von österreichischen Unternehmen herausfinden, ob Anwendungsbeispiele in ihrem Unternehmen schon sinnvoll einzusetzen sind – Stichwort unreife Technologie? Wie lange sollte man noch warten?

---

1. Was ist der Unterschied zwischen digitalem Fingerabdruck und digitaler Signatur?

Mit dem Fingerabdruck („Hashwert") wird ein eindeutiger Identifikator für Daten errechnet, mit dem man jedoch nicht auf die Daten "zurückrechnen" kann. Man kann den Hashwert veröffentlichen und damit später nachweisen, dass die Daten seit dem Veröffentlichungszeitpunkt nicht geändert wurden.

Mit der digitalen Signatur werden Daten "unterschrieben". Dabei wird bewiesen, dass der Verfüger einen bestimmten "privaten Schlüssel" benutzt hat, zu dem ein bestimmter "öffentlicher Schlüssel" gehört.

2. Warum haben Sie genau das Modell von Wüst et al. verwendet? Es gibt mittlerweile schon einige "Entscheidungsbäume" die alle Ihre Vor und Nachteile haben.

Aufgrund der beschränkten Zeit. Im Modell von Wüst et al, sind die wichtigsten Punkte enthalten, und die darin verwendeten Begriffe wurden im ersten Teil des Webinars bereits eingeführt. Die Verwendung anderer Modelle wie etwa

Klein, Sandra, and Wolfgang Prinz. "A Use Case Identification Framework and Use Case Canvas for identifying and exploring relevant Blockchain opportunities." *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET), 2018.

hätte mehr Zeit gebraucht, die dann bei den anderen Inhalten gefehlt hätte.

3. Gibt es schon Überlegungen die Software-Qualität der unterschiedlichen Blockchain-Technologien bzw. -Module sicherzustellen bzw. zu standardisieren?

Die Software-Qualität im Blockchainbereich ist derzeit ein aktives Forschungsgebiet. Im Rahmen des vor kurzem genehmigten K1 Centers Austrian Blockchain Center (https://blockchain-center.at/) werden entsprechende Projekte aufgesetzt, Federführend sind SBA-Research, TU und Uni Wien, TU Graz und IST.

4. Was sind NODES? Wie funktionieren diese?

Ein Node ist ein Computer, auf dem die jeweilige Blockchain-Software läuft. Alle Nodes schließen sich zu einem Peer To Peer Netz zusammen und tauschen die Transaktionen und die Blöcke aus.

Ein "Full-Node" speichert alle Daten einer Blockchain, es gibt auch Nodes, die nur Teile speichern. Nodes sind grundsätzlich gleichberechtigt, d.h. es gibt keine "zentralen" Nodes – wie z. B. bei einem Client-Server System.

5. Wie verhält es sich mit den immer wieder angesprochenen hohen Energieverbräuchen bei Blockchain-Anwendungen?

Den hohen Stromverbrauch gibt es bei sog. "Proof of Work" Blockchains (z. B. Bitcoin, Ethereum ...). Bei (modernen) Blockchain-Anwendungen, die auf anderen Verfahren basieren, gibt es keinen unnötig hohen Stromverbrauch mehr. Auch laufen Forschungen um weitere Verfahren zu entwickeln.

6. Wie gehe ich mit persönlichen Daten auf der Blockchain um (hinsichtlich DSGVO)?

Personenbezogene Daten können nicht direkt auf Blockchains gespeichert werden, da sie nicht mehr gelöscht werden könnten. Es gibt mehrere Verfahren, dieses Thema zu lösen. Eines ist das verschlüsselte Speichern, wobei sichergestellt werden muss, dass nur die betroffene Person selbst über den privaten Schlüssel verfügt und die Daten zu entschlüsseln bzw. nach Vernichten des privaten Schlüssels die Daten gar nicht mehr entschlüsselt werden können.

Ein zweiter Ansatz ist, die Daten nicht in einer Blockchain zu speichern sondern in einem anderen System (z. B. Datenbank, Filesystem) und in der Blockchain lediglich einen Link zu den Daten und einen Hashwert der Daten, um die Unmanipuliertheit sicherzustellen. Wenn die Daten gelöscht werden, dann geht der Link "ins Leere" und die Daten können nicht mehr gelesen werden.

7. Wie beurteilen Sie die Blockchain im Licht der EU-DSGVO (Unveränderbarkeit der Blockchain vs. 'Recht auf Vergessen werden' in der DSGVO)?

Siehe Frage 6.

8. Wenn ich Daten auf der Blockchain freigebe, wäre es ja für den Leser möglich, diese Informationen zu kopieren und für sich zu nutzen. Ist das möglich?

Wenn es sich um eine öffentlich lesbare Blockchain handelt, dann ja. Daten, die nicht öffentlich lesbar sein sollen, müssen verschlüsselt werden oder "offchain" transportiert werden. Siehe auch Frage 6.

9. Zum Beispiel Diebstahl: Wie wird verifiziert, dass der Diebstahl "echt" war? Risiko missbräuchliche Schädigung in Chains?

Siehe Frage 10.

10. Wie wird bei Everledger das Zertifikat beim Kauf an den Kunden übergeben? Und was würde im Fall des Verlusts dieses Zertifikats passieren? Eine Identifikation ist in diesem Fall nicht mehr möglich und somit kann ein eventueller Diebstahl nicht validiert werden.

Generell geht man bei derartigen Anwendungen wie folgt vor: Beim Kauf registriert man das Asset und das Zertifikat in der Blockchain, indem der Fingerprint des Assets und des Zertifikats mit dem öffentlichen Schlüssel des Käufers und dem privaten Schlüssel des Verkäufers verschlüsselt wird.

Verliert man das Zertifikat, kann man durch Entschlüsseln mit dem eigenen privaten Schlüssel und dem öffentlichen Schlüssel des Verkäufers beweisen, dass man es zum Zeitpunkt des Kaufes hatte und dass es nicht modifiziert wurde und in der realen Welt ein Duplikat anfordern.

In analoger Art und Weise kann man einen Diebstahl des Assets melden. Ein Dieb, der neben dem Asset auch das Zertifikat auf Papier erhalten hat, kann hingegen mangels Kenntnis des privaten Schlüssels einem neuen Käufer nicht nachweisen, dass er der rechtmäßige Eigentümer ist.

11. Werden sich die "Währungen" wie BTC durchsetzen oder werden sie verschwinden?

Meiner Ansicht nach werden sich Kryptowährungen stark verbreiten und in vielen Bereichen eingesetzt werden, da sie viele Vorteile haben. Ob das Bitcoin in der heutigen Form sein wird, bezweifele ich eher, da in den letzten Jahren viele (technische) Verbesserungspotentiale erkannt wurden.

12. Macht Mining noch Sinn oder gibt es für die Zukunft Alternativen?

Mining in der heutigen Form macht nur dann (wirtschaftlich) Sinn, wenn man über einen extrem niedrigen Strompreis verfügt. Gegenwärtig gibt es bereits Alternativen zum "Proof Of Work" bzw. wird an weiteren Alternativen geforscht. Vgl. auch Frage 5.

13. Kann die Kryptowährung bzw. Blockchain die nächste "Tulpenkrise" hervorrufen?

Die Gefahr einer durch eine Blase bei Kryptowährungen hervorgerufenen neuen Lehmankrise ist gering. Die Marktkapitalisierung von Kryptowährungen ist im Vergleich zu klassischen Finanzanlagen gering und es gibt keine Verflechtungen zur Realwirtschaft wie etwa Hypotheken. Die Blockchaintechnologie selbst ist vielfältig einsetzbar und viele Anwendungen haben mit Spekulationen nichts zu tun.

14. Wo kann ein Unternehmer in der Praxis konkret die Blockchain anwenden? Sind das gewisse Software-Programme?

Eine Blockchain ist eine neue Art von Datenbank, in der nicht Informationen, sondern Werte gespeichert und sicher übertragen werden können. Es gibt vielfältige Einsatzmöglichkeiten, einige wurden im Webinar vorgestellt. Blockchains werden also (wie z. B. auch eine Datenbank) als Technologie verwendet und von anderen Programmen "im Hintergrund" verwendet.

15. Was an der Blockchain Technologie ist speziell für KMU von Bedeutung/von Nutzen?

Für KMUs ist insbesondere die Möglichkeit rasch und billig Datenbestände zu notarifizieren ein Vorteil. Man kann dadurch ohne viel Aufwand sicher und bequem mit Geschäftspartnern, zu denen kein Vertrauen besteht, in Verbindung treten.

16. Welche Innovationen sind insgesamt mit dieser Technologie denkbar (abgesehen von Kryptowährungen)?

Es sind alle Anwendungen denkbar, bei denen es darum geht, Informationen bzw. Abbildungen von Werten dezentral und ohne Notwendigkeit von Vertrauen zu übertragen bzw. speichern.

17. Ist die Blockchain auch dafür geeignet, eine Cloud zu ersetzen, wo z.B. Kunden sensible Daten ablegen könnten?

Nein. Eine Blockchain ist mit einer Cloud nicht zu vergleichen und kann sie daher auch nicht ersetzen. Es besteht natürlich die Möglichkeit, Blockchain Software (sog. Nodes) als Cloudservice zu betreiben, was auch heute bereits von einigen Cloudanbietern gemacht wird.

18. Sind bereits touristische Anwendungen bekannt abseits der Flugverspätungs-Auszahlung?

Ja, es gibt folgende Anwendungsmöglichkeiten:

- Effizientere Kundenbindungsprogramme mit Kryptowährungen
- Real-Time Tracking von Gepäck (analog zum Everledger Case im Webinar)
- Dezentrale Alternativen zu Buchungsplattformen wie booking.com (z. B. https://windingtree.com/)

19. Welche Anwendungsbeispiele fallen Ihnen für die Baubranche ein? Gibt es schon welche, international?

Es gibt eine Fülle von Anwendungsmöglichkeiten neben der im Webinar bereits genannten Anwendung zur Erhöhung der Transparenz von Bauprojekten. Einen guten Überblock bietet https://laxary.de/blockchain/blockchain-bausektor

20. Wo sind die größten Hürden beim Einstieg in die Blockchaintechnologie?

Das Know-how – man muss sowohl die Technologie verstehen als auch das Geschäftsproblem. Pain Point Nummer 2 ist die noch unreife Technologie und das weitgehende Fehlen von Standards.

21. Ist der Einstieg in Blockchain eine Angelegenheit, die von den IT-Experten eines Unternehmens allein getroffen werden kann, oder ist dies eher "Chefsache" (Steuerung durch Geschäftsleitung)?

Ohne Geschäftsleitung kann man nicht in die Blockchain-Welt einsteigen. Es geht um bisher nicht IT-mäßig unterstützte Prozesse, insb. um den Austausch mit anderen Stakeholdern. Diese Bereiche anzugehen ist nur gemeinsam mit dem Management möglich.

22. Wie können CIOs von österreichischen Unternehmen herausfinden, ob Anwendungsbeispiele in ihrem Unternehmen schon sinnvoll einzusetzen sind – Stichwort unreife Technologie? Wie lange sollte man noch warten?

Wir raten dazu, auf keinen Fall zu warten, sondern jetzt beginnen, im kleinen Rahmen einen Prototyp zu bauen um die Technologie zu lernen und erste Erfahrungen zu sammeln. Denn: "Wenn man wartet, verpasst man den Anschluss."

Viele Unternehmen, die Partner im Austrian Blockchain Center sind, haben bereits Prototypen und Proofs of Concept durchgeführt.

Stand: 14.12.2018