Energieforschungsprogramm

Publizierbarer Endbericht

Programmsteuerung:
Klima- und Energiefonds

Programmabwicklung:
Österreichische Forschungsförderungsgesellschaft mbH (FFG)

Endbericht
erstellt am
30/06/2019

Projekttitel: Prosumer- und Nutzeranbindungim Verteilnetz mittels Blockchain [ProChain]

Projektnummer: 865082

Ausschreibung	4. Ausschreibung Energieforschungsprogramm
Projektstart	01/02/2018
Projektende	31/03/2019
Gesamtprojektdauer (in Monaten)	14 Monate
ProjektnehmerIn (Institution)	FH Salzburg, Zentrum für sichere Energieinformatik
AnsprechpartnerIn	Dominik Engel
Postadresse	Urstein Süd 1
Telefon	+43 050 2211 1305
Fax	
E-mail	office.zse@fh-salzburg.ac.at
Website	www.fh-salzburg.ac.at/zse

Prosumer- und Nutzeranbindungim Verteilnetz mittels Blockchain [ProChain]

AutorInnen:
Clemens Brunner, Dominik Engel, Andreas Unterweger, Fabian Knirsch – FH Salzburg
Andreas Sackl, Peter Fröhlich, Alexander Dimitrov – Austrian Institute of Technology

Beiträge und Diskussion der Unternehmenspartner werden dankend anerkannt.

1 Inhaltsverzeichnis

1 Inhaltsverzeichnis 4
2 Einleitung 5
3 Inhaltliche Darstellung 6
4 Ergebnisse und Schlussfolgerungen 9
5 Ausblick und Empfehlungen 13
6 Literaturverzeichnis 14
7 Anhang 16
8 Kontaktdaten 16

2 Einleitung

Blockchains werden als Schlüsseltechnologie im Bereich digitalisierter Energiesysteme gesehen (z.B. PwC Studie, „Revolutioniert Blockchain den Energiesektor?“, 2016 oder auch Bloomberg, „Gridchain: will blockchain work in the energy sector?“, 2016). Neben allen Vorteilen dieser Technologie ist eine differenzierte, kritische und systematische Bewertung notwendig. Das Projekt ProChain hat sich einer solche Bewertung für den Einsatz von Blockchain-Technologie in der Kundendomäne gewidment.
Gerade im Bereich der Anbindung von Endkundinnen und Endkunden ist eine detaillierte Bewertung der passenden Einsatzgebiete von Blockchain-Technologie essentiell, besonders hinsichtlich der Benutzerakzeptanz. Darüber hinaus spielen gerade im Endnutzerbereich, in dem kundenbezogene Daten verarbeitet werden, Datenschutz und damit auch Datensicherheit eine entscheidende Rolle.
Projekt ProChain hat den Einsatz von Blockchains zur Prosumer- und Nutzeranbindung im Verteilnetz anhand konkreter Anwendungsfälle untersuchen (*Mieterstrommodell*, *Eigenverbrauchsoptimierung* und *Electric Vehicle Charging)*. Generelle Anforderungen für den Einsatz von Blockchains, besonders hinsichtlich Wirtschaftlichkeit, Datenschutz und -sicherheit, Benutzerinteraktion, Datenhaltung und passende Blockchainmodelle, wurden für die Endanwenderdomäne abgeleitet. Im Speziellen wurden folgende Punkte adressiert:

1) Eignung verschiedener Blockchainansätze (private, public, hybrid; Consensus Algorithmen, Smart Contracts, etc.)
2) Anforderungen in Datenschutz und Datensicherheit
3) Anforderungen für Nutzerakzeptanz und für die Nutzerschnittstelle

Basierend auf den Anwendungsfällen wurden allgemeine Schlüsse und Empfehlungen erstellt. Eine Forschungsagenda wurde skizziert, welche Methoden und Ansätze aus den Erkenntnissen der Sondierung entwickelt (geeignete Blockchainansätze, Methoden für Datenschutz – *privacy enhancing technologies*, IT-Sicherheit, Nutzerakzeptanz und -anbindung). Folgende Beiträge wurden vom Sondierungsprojekt geleistet:

- Systematische Bewertung der Implikationen des Einsatzes von Blockchain-Technologie im Endnutzerbereich anhand verschiedener Parameter und am Beispiel konkreter Anwendungsfälle
- Bewertung der Auswirkungen von blockchain-basierter Nutzeranbindung auf Datenschutz und Datensicherheit
- Erhebung möglicher Methoden um Datenschutz für die Verarbeitung sensibler kundenbezogener Daten zu gewährleisten
- Gegenüberstellung und Bewertung verschiedener Modelle zum Betrieb von Blockchains (z.B. private Blockchains, öffentliche Blockchains, Consortium Blockchains; Validierungskonzepte, sowie verschiedene Mechanismen zur Abbildung der Businesslogik), sowie die Möglichkeit ihrer Verbindung in einem hybriden Modell
- Erste Erhebungen von Anforderungen für Nutzerakzeptanz von Blockchain-Technlogie und der Anforderungen für die Schnittstelle zum Nutzer

Die gesteckten Ziele wurden vom Projekt erreicht. Speziell im Bereich der Benutzeranforderungen, Datenschutz und Datensicherheit konnten wesentliche Erkenntnisse erzielt werden.

3 Inhaltliche Darstellung

Blockchain-Technologie wurde 2008 für die digitale Währung „Bitcoin“ erstmals vorgeschlagen (Nakamoto08). Die Blockchain für Bitcoin dient hierbei als dezentrale Datenbank für Transaktionen und bildet somit verteilt den Zustand der Konten aller Teilnehmer ab. Basierend auf dem Bitcoin-Protokoll sind mittlerweile zahlreiche Abspaltungen für digitale Währungen entstanden (z.B. Lite Coin, Zero Cash, etc.). Daraus weiterentwickelt wurden Smart Contracts in einer Blockchain (z.B. Ethereum, Wood17a). Smart Contracts in Verbindung mit Blockchains erlauben das verteilte und nachweisbare Ausführen von komplexen, selbstständigen (Turing-vollständigen) Berechnungen.
Neben den genannten Ausprägungen ist auch der Consensus-Algorithmus ein entscheidendes Merkmal einer konkreten Blockchain-Technologie. Aktuelle Implementierungen verwenden dafür Proof-of-Work (PoW), Proof-of-Stake (PoS), künftig auch Proof-of-Authority (PoA) oder hybride Ansätze (z.B. Polkadot).
Bei PoW wird der Consensus durch das Lösen eines mit bestimmtem Rechenaufwand verbundenen Problems erreicht (Nakamoto08, Wood17a). Dies ist in der Regel das Berechnen einer kryptografischen Hashfunktion, wobei die Ausgabe in einen bestimmten Wertebereich fallen muss.
Bei PoS wird dieser energieaufwändige Consensus-Algorithmus durch den Nachweis des Haltens einer bestimmten Menge von Einheiten der zugrundeliegenden digitalen Währung ersetzt. Das Recht, einen neuen Block zu erzeugen, wird mit bestimmter Wahrscheinlichkeit anteilsmäßig an die sog. Stakes vergeben (Croman16, Tschorsch16). Die Eintrittshürde steigt damit mit jedem neuen Teilnehmer, reduziert jedoch deutlich den Energieaufwand.

Ein weiterer Ansatz zur Reduktion des Rechenaufwandes ist PoA. Dabei haben ausschließlich bestimmte Knoten des dezentralen Netzwerkes das Recht neue Blöcke zu erzeugen. Hierzu ist jedoch ein Vertrauen in diese Teilnehmer erforderlich (Dinh17).
Erste Ansätze für hybride Modelle, wie etwa Polkadot (Wood17b), zielen auf eine übergreifende Kommunikation zwischen Blockchains mit verschiedenen Consensus-Algorithmen (PoW, PoS, PoA).

Blockchain-Technologie wird auch bereits am freien nationalen und internationalen Markt für Produkte verwendet. Beispielhaft seien hier genannt:

- HEROcoin (Österreich): Als Plattform für Onlinesportwetten u.dgl. wird die dezentrale Architektur einer Blockchain verwendet. Darüber hinaus werden Wetteinsätze und die entsprechenden Auszahlungen über blockchain-basierte Zahlungsmittel (Herocoin) repräsentiert (https://s3-cdn.herocoin.io/HERO_Whitepaper.pdf)
- slock.it (Deutschland): Als Kombination vom Internet der Dinge (IoT) und Blockchain-Technologie werden so genannte intelligente Objekte ermöglicht, die Verträge abschließen können, z.B. das Leasing nicht vollständig ausgelasteter Elektrofahrzeuge. Die Umsetzung bedient sich dabei der blockchain-basierten Smart Contracts. (https://slock.it/)

- Ethereum (Schweiz): Etherum verfolgt das Ziel einer Smart Economy. Mit Hilfe von öffentlicher Blockchain-Technologie und Smart Contracts ist es möglich, die Verwaltung digitaler Assets ohne Notar dezentral und transparent zu ermöglichen.

Allgemein dient Blockchain-Technologie dazu, Informationen dezentral, nachträglich unveränderbar und dauerhaft zu speichern, was unter anderem den digitalen Transfer von Assets ermöglicht.
Damit ergeben sich zahlreiche Anwendungsgebiete, wo digitale Währungen ein erster Eintrittspunkt waren. Hierbei sind die Interaktion der Benutzerinnen und Benutzer sowie eine differenzierte Auseinandersetzung mit den Anforderungen an Sicherheit, Datenschutz und dem Einsatzgebiet von großer Bedeutung (Delmolino16, Croman17). Weitere Entwicklungen beschäftigen sich mit der Verbesserung der Privatsphäre in Blockchains, z.B. ZeroCash (Zyskind14), Hawk (Ben-Sasson14). Es lassen sich folgende Anwendungsfälle für Blockchain-Technolgie (zusätzlich zu den oben genannten, sich auf dem Markt befindlichen) aus der Literatur ableiten, die allesamt die Rolle als Schlüsseltechnologie in der Energiewirtschaft unterstreichen:

- Digitale Währungen (z.B. Nakamoto08, Zyskind14, Peters16)
- Smart Contracts (z.B. Wood17a)
- Internet of Things (z.B. Christidis16)
- Smart Grid (z.B. Knirsch17a)
- Electric Vehicles (z.B. Knirsch18, Knirsch17c, Dubois17)

Die Energy Web Foundation (http://energyweb.org/) hat insgesamt knapp 100 Anwendungsfälle identifiziert. Insbesondere das Querschnittsthema der Integration digitaler Währungen und *Smart Contracts* in das Internet of Things, das Smart Grid und in Electric Vehicles ergibt eine Vielzahl neuer Anwendungsfälle.
Beispiele für solche erweiterten Anwendungsfälle mit Bezug zur Kundenintegration, der erreichten Sicherheit und der Erhaltung der Privatsphäre werden an der Fachhochschule Salzburg für den Energiebereich (insbesondere für Smart Grid und Electric Vehicles) erarbeitet:

- Finden optimaler Tarife für verschiedene Verbrauchsgruppen unter Wahrung der Privatsphäre im Smart Grid (Unterweger16)
- Tarifauswahl im Smart Grid unter Wahrung der Privatsphäre mit Smart Contracts in einer Blockchain (Knirsch17a)
- Laden von Elektrofahrzeugen mit Auswahl des optimalen Tarifs (Knirsch18, Knirsch17c, Dubois17)
- Transparente Energieanbieter-Tarifauswahl mittels Ethereum und Blockchain-Technologie (Leixnering17)

Zur Nutzerakzeptanz von Blockchain-Technologie wurde bisher nur wenig Forschung durchgeführt. So hat beispielsweise [Folkinshteyn16] das sogenannte Technology Acceptance Model [Venkatesh08] angewendet, um die Akzeptanz der Blockchain-Technologie im Kontext von Kryptowährungen wie etwa Bitcoin zu erforschen. Die grundlegende Blockchain-Technologie wurde einerseits positiv bewertet (z.B. erhöht wahrgenommene Ausfallsicherheit durch Dezentralisierung), allerdings empfanden potentielle Nutzer die Technik auch als riskant (z.B. wurde angemerkt, dass Fehler – verursacht durch falsche Überweisungen, kriminelle Aktivitäten, etc. – in der Transaktionshistorie nachträglich nicht mehr geändert werden können). Es wird außerdem betont, dass die Darstellung von (abstrakten) Konzepten,

wie etwa der Blockchain-Architektur und kryptografische Verfahren auf die jeweilige Zielgruppe angepasst sein muss.

Die konkrete Gestaltung der Anbindung von Blockchain-Technologie an Anwendungen und deren Präsentation im User Interface sollte als ein wichtiger Erfolgsfaktor betrachtet werden. Allerdings sind viele Fragen der Kundenanbindung bisher noch unzureichend adressiert worden. Es gibt erste Hinweise aus der Praxis [Baker-Mill17], welche Design-Prinzipien besonders wichtig sein könnten – diese sind aber noch weit davon entfernt, als gesicherte Erkenntnisse gelten zu können. Eine grundlegende Frage der Gestaltung besteht darin, wieviel der zugrundeliegenden Daten und Transaktionen den NutzerInnen überhaupt angezeigt werden sollen. Diese Basisinformationen könnten einerseits verwirrend, überlastend oder störend sein; andererseits könnten sie auch zu mehr Vertrauen beitragen. Ein ähnliches, bisher noch nicht aufgelöstes Dilemma zeigt sich in der Entscheidung, wieviel Eingriffs- und Kontrollmöglichkeiten Nutzer in den zugrundeliegenden Blockchain-Prozessen haben sollten.

Die Verwendung von Blockchain-Technologie für Anwendungsfälle in der Energiewirtschaft muss dabei auf besondere Aspekte und Herausforderungen der Branche Rücksicht nehmen. Dabei spielen vor allem die Anforderungen und die Akzeptanz der Nutzerinnen und Nutzer hinsichtlich Steuerung und insbesondere Datenschutz eine bedeutende Rolle (Delmolino16, Ben-Sasson14). Auch hinsichtlich der Skalierbarkeit der Lösung betreffend Datenmengen, Durchsatz und Anzahl der Nutzerinnen und Nutzer (Croman16, Tschorsch16) muss für diese Domäne noch eine Bewertung erfolgen.

Blockchain-Technologie bietet eine Vielzahl neuer Chancen in Bezug auf dezentrale Speicherung von Daten, der Reduktion des erforderlichen Vertrauens und der permanenten, nachträglich unveränderbaren Datenhaltung. Diese Vorteile können jedoch auf Kosten der Skalierbarkeit (Croman16), der Privatsphäre (Reid13) oder des Kommunikationsaufwands (Tschorsch16) entstehen. Die Verwendung der Technologie in neuen Anwendungsfällen konkurriert deshalb mit konventionellen, zentralisierten Lösungen. Diesen konventionellen Ansätzen ist der Nutzen der neuen Technologie gegenüberzustellen:

- Reduziertes Vertrauen zwischen den Teilnehmern aufgrund des dezentralen Consensus
- Ausfallssicherheit durch Verteilung der Daten über alle Teilnehmer
- Nachträgliche Unveränderbarkeit und somit Unabstreitbarkeit einmal hinzugefügter Daten
- Direkte Integration und Anbindung von Nutzerinnen und Nutzer ohne zentrale kontrollierende Instanz

Darüber hinaus lässt sich die Blockchain-Technologie aufgrund zahlreicher Variationsmöglichkeiten in Bezug auf Consensus-Algorithmus, des Nutzerinnen- und Nutzerkreises (privat, öffentlich oder hybrid) und der Ausprägung (reine Datenhaltung, Transaktionen oder Smart Contracts) sehr granular an die Domäne und den jeweiligen Anwendungsfall anpassen.

Eine differenzierte Betrachtung der Eignung von verschiedenen Spielarten der Blockchain-Technologie im Verteilnetz und ihrer Wirtschaftlichkeit, ihrer Auswirkung auf Datenschutz und Datensicherheit, sowie ihrer Akzeptanz bei den Endanwenderinnen und Endanwendern fehlt bis dato – weder auf theoretischer

Ebene noch in Bezug auf konkrete Proof of Concepts gibt es dazu Berichte. Das vorliegende Projekt adressierte diese Lücke.

4 Ergebnisse und Schlussfolgerungen

Diese Betrachtung erfolgte anhand drei exemplarisch gewählter Use Cases, wobei zunächst eine Literaturrecherche zum State of the Art erfolgt und danach eine prototypische Implementierung für ausgewählte Aspekte. Diese dient der Gegenüberstellung von konventionellen Ansätzen und Blockchain-Technologie und der Bewertung von sozioökonomische Aspekte und Datenschutzimplikationen.
Die folgenden Anwendungsfälle wurden in ProChain betrachtet:

- Mieterstrommodell
- Eigenverbrauchsoptimierung/Demand Response Management
- Electric Vehicle Charging
- Energieherkunftsnachweise

Alle Anwendungsfälle haben gemeinsam, dass mehrere, heterogene TeilnehmerInnen einen gemeinsamen Zustand (z.B. Aufteilungsschlüssel einer PV-Anlage) abbilden wollen. Dieser Zustand soll transparent, nachvollziehbar und unveränderbar sein. Blockchaintechnologie bietet sich in diesem Fall daher grundsätzlich an (Wüst17). Trotz dieser prinzipiellen Eignung soll in diesem AP jedoch geklärt werden, ob auch sozioökonomische Faktoren für einen Einsatz sprechen. Im Folgenden findet sich eine Zusammenfassung der Erkenntnisse zu Vor- und Nachteile sowie Handlungsempfehlung für jeden der drei Use Cases. Eine Analyse des State of the Art, sowie klare Handlungsempfehlungen für Blockchainanwendungen unter exemplarischer Betrachtung des Anwendungsfalls „Mieterstrommodell“ wurden im Rahmen des Projekts erarbeitet und publiziert (Knirsch19).
Es wurden außerdem mehrere Workshops mit den Projektpartnern durchgeführt, um die Anforderungen an die Anwendungsfälle aus Sicht der Energiewirtschaft zu klären und um Rahmenbedingungen für die Bewertung der sozioökonomischen Faktoren bzw. der Bewertung der BenutzerInnenakzeptanz zu definieren.

Mieterstrommodell
Das Mieterstrommodell bzw. dessen Implementierung durch Netzbetreiber ist eine gesetzliche Anforderung. Die Umsetzung erlaubt BewohnerInnen von Mehrparteienhäusern mit einer PV-Anlage das (dynamische) Festlegen eines Aufteilungsschlüssels der Anteile an dieser PV-Anlage. Damit kann eine Partei zeitlich begrenzt Anteile an der PV-Anlage an andere Parteien übertragen. Die Aufteilung muss transparent und nachvollziehbar erfolgen. Da es mehrere schreibende Parteien gibt und ein gemeinsamer und nachträglich unveränderbarer Zustand (Anteile) gespeichert werden muss, bietet sich nach Wüst (Wüst17) der Einsatz einer privaten Blockchain an. Als Vorteil ist zu nennen, dass sich das Vertrauen (d.h. die Speicherung des gemeinsamen Zustands über alle Parteien) verteilt und die Parteien aktiv an der Sicherung der Daten teilnehmen können. Im Rahmen einer prototypischen Umsetzung wurde neben der Evaluierung dieser technischen Faktoren eine wirtschaftliche Betrachtung vollzogen,

sowie im Rahmen einer Nutzerstudie die sozioökonomischen Aspekte betrachtet. Zusammengefasst lässt sich feststellen, dass eine Blockchainlösung für das Mieterstrommodell prinzipiell geeignet ist, jedoch ein hoher Automatisierungsgrad auf Seiten der BenutzerInnen wünschenswert ist. Aus ökonomischer Sicht kann die Sicherung der Daten zwar auf alle Teilnehmer aufgeteilt werden, jedoch ist für die Abrechnung ein Abgleich mit zentraler Datenhaltung beim Netzbetreiber bzw. Energieanbieter notwendig. Die im Rahmen der Projektlaufzeit erfolgte detaillierte Ausgestaltung des Gesetzesentwurfs hat zu Änderungen in den Rahmenbedingungen geführt, die – zumindest für kleine Mehrparteienhäuser – eine einfache Implementierung auch ohne Blockchain erlauben, da der Netzbetreiber als zentrale vertrauenswürdige Instanz agieren kann.

Eigenverbrauchsoptimierung/Demand Response Management

Ziel der Eigenverbrauchsoptimierung ist es, die Energieerzeugung und den Energieverbrauch innerhalb einer geschlossenen Einheit (üblicherweise ein Haus) möglichst auszugleichen. In einem typischen Anwendungsfall verfügt ein Haus über eine PV-Anlage und möchte den Eigenverbrauch der erzeugten Energie maximieren. Die Betrachtung des Anwendungsfalls zeigt einen hohen Grad an Ähnlichkeit zum oben beschriebenen Miterstrommodell. Bei diesem wird eine Maximierung des Eigenverbrauchs über mehrere Parteien hinweg angestrebt. Ein ähnlicher Ansatz wird in Local Energy Communities verfolgt (Mengelkamp18a, Mengelkamp18b). Hier finden sich in der Literatur Vorschläge zur Umsetzung der Optimierung (unter Verwendung monetärer Anreizsysteme) aus Basis von Blockchaintechnologie. Zusammengefasst kann als Handlungsempfehlung gegeben werden, dass Blockchaintechnologie dann vorteilhaft einsetzbar ist, wenn eine Optimierung über mehrere Haushalte hinweg erfolgt und eine große Zahl schreibender Parteien existiert. Für die Optimierung innerhalb eines Haushalts können leichtgewichtige, zentralisierte Lösungen verwendet werden.

Electric Vehicle Charging

Dieser Anwendungsfall umfasst das Laden von Elektrofahrzeugen, wobei hier einerseits der Austausch der Energie und andererseits die Wahl der Ladesäule als Anwendungsfall betrachtet werden kann. Letzteres ist von Knirsch et al. (Knirsch18) detailliert beschrieben und legt die Vor- und Nachteile der Blockchain dar. Für ersteren Fall kann wiederum die Analogie zu den oben beschrieben Anwendungsfällen gezogen werden. Bei Betrachtung des Elektrofahrzeugs als Speicher und bei Einbettung in ein heterogenes, dezentralisiertes System von Teilnehmern in einer Local Energy Community kann eine Blockchainlösung das Potenzial zu einer transparenten und nachvollziehbaren Abbildung von Energieanteilen verwendet werden.

Vergleich verschiedener Blockchainansätze

Durch Knirsch et al. (Knirsch2019) wurde am Beispiel des Mieterstrommodells die Verwendung verschiedener Blockchainansätze (private, public) mit verschiedenen Consensus-Algorithmen - Proof of Work (PoW), Proof of Stake (PoS) und Proof of Authority (PoA) – im Detail untersucht. Es wurden verschiedene verfügbare Implementierungen dieser Ansätze und Consensus-Algorithmen verglichen und gegenübergestellt. Es wurde außerdem eine eigene PoW-basierte, private-permissioned-Blockchain implementiert und bewertet, die in Testhaushalten in Salzburg zum Einsatz kam. Darüber hinaus wurde

auf Grund der Weiterentwicklung des State of the Art festgestellt, dass eine solche Implementierung per Stand Projektende wirtschaftlicher (da energiesparender) möglich wäre, da es große Fortschritte in der Skalierbarkeit im Bereich der BFT-Algorithmen (als Ersatz für die oben genannten Consensus-Mechanismen) gab.
In den Testhaushalten, in denen die oben genannte Eigenimplementierung einer Blockchain inkl. grafischer Benutzeroberfläche für Endanwender sechs Monate im Einsatz war, wurden neben der Umsetzung des Mieterstrommodells die Verwendung von Speichermöglichkeiten berücksichtigt, da eine der Kundenanlagen über einen Speicher für Solarenergie verfügte. Darüber hinaus wurde das Laden von Elektrofahrzeugen und Speichermanagement mitberücksichtigt, da den Haushalten ein Elektrofahrzeug zur Verfügung stand, dessen Ladesäule über die Solaranlage mitgespeist wurde und von den mieterstrombedingten Verschiebungen profitieren konnte.
Die Eigenverbrauchsoptimierung wurde in einem Testaufbau für einen fiktiven Haushalt in Niederösterreich basierend auf Echtdaten in Form eines implementierten Prototypen berücksichtigt.
Wie von Wüst (Wüst17) bereits ausgeführt, ist die Verwendung von Blockchains für die drei genannten Anwendungsfälle im Allgemeinen sowie die konkrete Verwendung einzelner Ansätze und Consensus-Algorithmen im Speziellen wie folgt zu bewerten: In Anwendungen, bei denen mehrere Endanwender gleichzeitig Zustände dezentral speichern möchten und wo es keine zentrale vertrauenswürdige Partei gibt, ist die Verwendung einer Blockchain nicht sinnvoll. Ebensowenig ist eine Blockchain sinnvoll, wenn sich alle Parteien gegenseitig vertrauen. Ist es notwendig, dass alle Transaktionen öffentlich überprüft werden (über die beteiligten Parteien hinaus), ist eine public permissioned Blockchain sinnvoll, in der einzelne Parteien über Schreibrechte verfügen, aber jeder Teilnehmer Daten lesen und überprüfen kann. Ist keine derartige öffentliche Überprüfung notwendig oder sinnvoll und nur die teilnehmenden Parteien benötigen Zugriff zur Verifikation (z.B. Mieterstrommodell ohne Berücksichtigung des Netzbetreibers), ist eine private permissioned Blockchain sinnvoll, deren Teilnehmerkreis beschränkt ist. Eine solche Implementierung wird von Knirsch et al. (Knirsch2019) im Rahmen von ProChain im Detail beschrieben.
Ziel von ProChain war, die Auswirkungen auf Privatsphäre und Security bei der Umsetzung von Anwendungsfällen mittels Blockchaintechnologie zu evaluieren. Dabei wird nicht nur der Einfluss der unveränderbaren Datenhaltung auf die Privatsphäre der BenutzerInnen erhoben, sondern auch wie die Sicherheit der Daten gewährleistet werden kann. Die Fragestellung lässt sich in zwei Teile gliedern:

- Privacy: Umfasst Methoden für Datenschutz aus BenutzerInnensicht.
- Security: Umfasst den Schutz der Daten vor nachträglicher Veränderung.

Letzteres ist eine der Haupteigenschaften der Blockchaintechnologie. Durch die Verwendung kryptografischer Methode (Hashfunktionen und Signaturen) wird sichergestellt, dass nachträgliche Änderungen an den Daten einzelner, bestätigter Transaktionen nicht bzw. nur mit unverhältnismäßig hohem Aufwand möglich sind (Nakamoto08).

Neben der Manipulation von Daten, die bei der Anwendung von Blockchaintechnologie aus den oben genannten Gründen nicht möglich ist, sind verschiedene weitere Angriffe bekannt. Diese umfassen beispielsweise die Eclipse-Attacke (Karlsson18) oder die unter bestimmten Umständen mögliche Rechenleistungsübernahme mit geringem Anteil (Eyal14,Knirsch18).

Die Unveränderbarkeit von Daten ist ein zentrales Kriterium für die Wahl von Blockchaintechnologie für die Umsetzung vieler Anwendungsfälle, wie etwa die in diesem Projekt analysierten (Mieterstrommodell, Eigenverbrauchsoptimierung, Elektrofahrzeuge). Dies impliziert jedoch die Notwendigkeit einer klaren Abwägung der Vor- und Nachteile dieser permanenten Speicherung von (möglicherweise) personenbezogenen Daten.

Die Datenanalyse der anfallenden Nutzerdaten zeigt, dass je nach Anwendungsfall eine Mindestmenge personenbezogener Daten für den Betrieb notwendig ist. Im Falle des Mieterstrommodells ist dies die Zuordnung einer Partei die Anteilseigner einer Solarstromanalage ist zu den jeweiligen Anteilen (Knirsch19). Für die vorgeschlagene Umsetzung wurde daher eine private permissioned Blockchain gewählt in der die Zugriffsrechte (lesend und schreiben) auf die Teilnehmer und den Netzbetreiber eingeschränkt sind. Diese müssen den Verteilschlüssel jederzeit einsehen und auf Basis ihrer Rechte modifizieren können.

Als mögliche Lösung im Elektrofahrzeuganwendungsfall wurde in ProChain die Verwendung sogenannter Commitments vorgeschlagen (Knirsch18, Unterweger18). Da in diesem Fall keine private permissioned, sondern eine public Blockchain verwendet wird, würden sonst alle personenbezogenen Daten (kritisch: Standort, Zuordnung von Ladestationsstandort zu BenutzerInnen) öffentlich einsehbar sein. Commitments sind privacy enhancing technologies, die auch in anderen Domänen breiten Einsatz finden (Knirsch18b, Delmolino16).

Für Eigenverbrauchsoptimierung ist eine genaue und transparente Aufzeichnung von Verbrauchs- und Erzeugungsleistungen notwendig. Dies kann beispielsweise über ein Zertifikatssystem (Brunner19) abgebildet werden. Hierbei werden anstatt der Daten selbst nur deren Hash auf der Blockchain registriert. Durch die kryptografischen Eigenschaften dieser Hashfunktionen (Unumkehrbarkeit) ist eine Zuordnung zu direkt personenbezogenen Daten ohne Kenntnis dieser nicht möglich.

Nutzerorienterte Vermittlung von Blockchain-basierten Diensten Entlang des Lifecycles der Verwendung einer Blockchain-basierten Anwendung wurden verschiedene Aspekte der Vermittlung von Blockchain-Aspekten und deren Einfluss auf das NutzerInnen-Erlebnis untersucht. In Bezug auf die Erwartungshaltung gegenüber Blockchain-Aspekten wurde die Präferenz zentraler Blockchain-Eigenschaften mit denen herkömmlicher Setups verglichen. Bei paarweisen Vergleichen stellte sich heraus, dass einige Eigenschaften, insbesondere die Abwesenheit (vs. der Anwesenheit) eines Intermediärs in Blockchain-basierten Anwendungen durchaus positiv von NutzerInnen gesehen werden. Weiters zeigte sich, dass die Art der Vermittlung dieser Eigenschaften einen starken Einfluss auf die Akzeptanz haben kann. So führte die Formulierung (bspw. dezentrale Verwaltung statt Speicherung) zu unterschiedlichen Präferenzen bei NutzerInnen. Auch machte der Betrag bzw die Dauer einer Transaktion durchaus einen Unterschied bei der Präferenz von Blockchain Eigenschaften: bei höheren Beträgen (1200 statt 25 EUR) wurde typischerweise die traditionelle Variante vorgezogen.
Weiters wurde ein Technologieakzeptanzmodell entwickelt und validiert. Es stellte sich dabei heraus, dass auch Komponenten wie wahrgenommene Nutzungsfreude und der wahrgenommene Innovationsgrad nicht zu vernachlässigende Determinanten für die intendierte zukünftige Nutzung sind.

Eine weitere wesentliche Erkenntnis der nutzerzentrierten Forschung in diesem Projekt ist, dass Blochchain-bezogene Informationen durchaus vertrauensschaffend sein kann und daher auch nicht per se versteckt werden müssen.

5 Ausblick und Empfehlungen

Zusammengefasst kann als Handlungsempfehlung zum Einsatz der Blockchaintechnologie abgeleitet werden:

- Es muss eine größere Anzahl verteilter und aktiv am Prozess teilnehmender Parteien geben und die Benennung einer zentralen, vertrauenswürdigen Instanz ist nicht sinnvoll oder möglich.
- Die Benutzerakzeptanz und der Automatisierungsgrad der Lösung müssen vor Einsatz der Blockchaintechnolgie klar evaluiert und betrachtet werden.
- Es muss für den Einsatz von Blockchainlösungen den Bedarf für transparente und nachvollziehbare Datenhaltung geben, dieser bedarf muss jedoch Fragen des Datenschutzes gegenübergestellt werden.
- Ökonomische Faktoren zum Aufsetzten und Verteilen der Knoten sowie zur Anreizbildung für das Betreiben von Knoten müssen klar gegenüber zentralen Lösungen abgewogen werden.

Da im Verteilnetz dem Energieversorger und dem Netzbetreiber eine große Vertrauensrolle als Betreiber kritischer Infrastruktur zukommt, sind reine Blockchainlösungen in vielen Fällen höchstwahrscheinlich nicht sinnvoll. Wie oben beschrieben, ist eine Blockchain bei Vorhandensein einer zentralen vertrauenswürdigen Instanz nicht notwendig. Im Mieterstrommodell jedoch kann die Einigung einer Eigentümergemeinschaft, wie in [1] ausgeführt, in Form einer private permissioned Blockchain widerspruchsfrei für den Netzbetreiber dokumentiert werden, auch wenn sich die einzelnen teilnehmenden Parteien nicht zwingend vertrauen.

Wie in dem Projekt vorangegangenen Arbeiten ausgeführt wurde, sind Datenschutz, Datensicherheit sowie die Verwendung von Smart Contracts im Hinblick auf Wirtschaftlichkeit (und vor allem Kosten) ausführlich und je Anwendungsfall zu bewerten. Wie beispielsweise von uns gezeigt wurde (Unterweger18, Unterweger17), ist das Implementieren von datenschutz- und datensicherheitsbewahrenden Protokollen zum Energietarifvergleich für Endkunden in Form von Ethereum-Smart-Contracts mit erheblichem Aufwand und Ausführungskosten verbunden. Ähnliche Feststellungen wurden auch in einem anderen Kontext gemacht (Knirsch18b). Von allen drei Publikationen wird eine überproportionale Kostensteigerung durch datenschutzerhaltende Mechanismen sowie eine größenabhängige Datenverarbeitungsgebühr festgestellt, die viele praktische Anwendungen erschwert oder gar unmöglich (da unwirtschaftlich) macht.

Diese Schlussfolgerungen lassen sich auf die in diesem Projekt vorliegenden Anwendungsfälle übertragen. Insbesondere wurde festgestellt, dass die Verwendung von datenschutzverbessernden Maßnahmen, insbesondere in Form von Smart Contracts, in Blockchainlösungen teurer umzusetzen sind als in klassischen Lösungen, wo die Übertragung und Verarbeitung von Daten im KB-Bereich keine Kosten im € oder 10€-Bereich nach sich zieht. Auch wenn Blockchains einige Datensicherheitseigenschaften (z.B. persistente chronologische und im Nachhinein nicht änderbare

Speicherung von Transaktionen) bereits implementieren, ist der weit verbreitete PoW-Consensus-Mechanismus auf Grund seines Energieverbrauches nicht wirtschaftlich (vgl. oben).
Zusammengefasst lässt sich nach Bewertung und Analyse der in der Literatur vorgeschlagenen Verfahren und im Kontext der im Rahmen des Projektes untersuchten Anwendungsfälle schlussfolgern, dass

- personenbezogene Daten in vielen Anwendungsfällen auf ein Minimum beschränkt werden können;
- selbst dieses Minimum an Daten mit weiteren privacy enhancing technologies vor unberechtigten Zugriffen geschützt werden kann;
- und dass die Blockchaintechnologie selbst über ihre intrinsischen Sicherheitsmechanismen vor Manipulation der Daten schützt.

6 Literaturverzeichnis

[Baker-Mills17] Sarah Baker Mills. “Blockchain Deisgn Principles”. In “Design at IBM”, accessed on 13 September 2017: https://medium.com/design-ibm/blockchain-design-principles-599c5c067b6e

[Ben-Sasson14] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, “Zerocash: Decentralized Anonymous Payments from Bitcoin,” in Proceedings -- IEEE Symposium on Security and Privacy, 2014, pp. 459–474.

[Brunner19] C. Brunner, F. Knirsch, and D. Engel, “SPROOF: A platform for issuing and verifying documents in a public blockchain,” in 5th International Conference on Information Systems and Privacy, 2019.

[Christidis16] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.

[Croman16] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Gün Sirer, D. Song, and R. Wattenhofer, “On Scaling Decentralized Blockchains,” in Financial Cryptography and Data Security: FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers, J. Clark, S. Meiklejohn, P. Y. A. Ryan, D. Wallach, M. Brenner, and K. Rohloff, Eds. Berlin Heidelberg: Springer Berlin Heidelberg, 2016, pp. 106–125.

[Delmolino16] K. Delmolino, M. Arnett, A. E. Kosba, A. Miller, and E. Shi, “Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab.,” in Financial Cryptography and Data Security, 2016, pp. 79–94.

[Dinh17] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, “BLOCKBENCH: A Framework for Analyzing Private Blockchains,” in SIGMOD ’17 Proceedings of the 2017 ACM International Conference on Management of Data, 2017, pp. 1085–1100.

[Dubois17] A. Dubois, A. Wehenkel, R. Fonteneau, F. Olivier, and D. Ernst, “An App-based Algorithmic Approach for Harvesting Local and Renewable Energy Using Electric Vehicles,” in Proceedings of the 9th International Conference on Agents and Artificial Intelligence (ICAART 2017), 2017.

[Eyal14] I. Eyal and E. G. Sirer, “Majority is not Enough: Bitcoin Mining is Vulnerable,” in Financial Cryptography and Data Security, 2014, pp. 436–454.
[Folkinshteyn16] D. Folkinshteyn, M. Lennon, “Braving Bitcoin: A technology acceptance model (TAM) analysis”, In: Journal of Information Technology Case and Application Research Vol. 18 , Iss. 4,2016
[Karlsson18] K. Karlsson, W. Jiang, S. Wicker, D. Adams, E. Ma, R. Van Renesse, and H. Weatherspoon, “Vegvisir: A partition-tolerant blockchain for the internet-of-things,” in International Conference on Distributed Computing Systems, 2018, pp. 1150–1158.
[Knirsch17a] F. Knirsch, A. Unterweger, G. Eibl, and D. Engel, “Privacy-Preserving Smart Grid Tariff Decisions with Blockchain-Based Smart Contracts,” in Sustainable Cloud and Energy Services: Principles and Practices, W. Rivera, Ed. Springer International Publishing, 2017. To appear.
[Knirsch18] F. Knirsch, A. Unterweger, and D. Engel, “Privacy-preserving Blockchain-based Electric Vehicle Charging with Dynamic Tariff Decisions,” J. Comput. Sci. - Res. Dev., vol. 33, no. 1, pp. 71–79, 2018.
[Knirsch18b] F. Knirsch, A. Unterweger, K. Karlsson, D. Engel, and S. B. Wicker, “Evaluation of a Blockchain-based Proof-of-Possession Implementation,” 2018-01, 2018.
[Knirsch19] F. Knirsch, A. Unterweger, and D. Engel, “Implementing a Blockchain from Scratch: Why, How, and What We Learned,” EURASIP J. Inf. Secur., 2019.
[Kosba16] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts,” in 2016 IEEE Symposium on Security and Privacy (SP), 2016, pp. 839–858.
[Leixnering17] C. Leixnering, “Transparente Energieanbieter-Tarifauswahl mittels Ethereum und Blockchain-Technologie,” Bachelor thesis, Fachhochschule Salzburg, 2017.
[Nakamoto08] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Bitcoin.org, pp. 1–9, 2008.
[Mengelkamp18a] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, “Designing microgrid energy markets: A case study: The Brooklyn Microgrid,” Appl. Energy, vol. 210, pp. 870–880, 2018.
[Mengelkamp 18b]´E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, “A blockchain-based smart grid: towards sustainable local energy markets,” Comput. Sci. - Res. Dev., vol. 33, no. 1, pp. 207–214, 2018.
[Peters16] G. W. Peters and E. Panayi, “Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money,” in Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty-First Century, T. Paolo, T. Aste, L. Pelizzon, and N. Perony, Eds. Cham: Springer International Publishing, 2016, pp. 239--278.
[Reid13] F. Reid and M. Harrigan, “An Analysis of Anonymity in the Bitcoin System,” in Security and Privacy in Social Networks, Y. Altshuler, Y. and Elovici, A. B. and Cremers, N. and Aharony, and A. and Pentland, Eds. Springer New York, 2013, pp. 197–223.
[Tschorsch16] F. Tschorsch and B. Scheuermann, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies,” IEEE Commun. Surv. & Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.
[Unterweger16a] A. Unterweger, F. Knirsch, G. Eibl, and D. Engel, “Privacy-preserving load profile matching for tariff decisions in smart grids,” EURASIP J. Inf. Secur., vol. 2016, no. 1, pp. 1–17, 2016.

[Unterweger17] A. Unterweger, F. Knirsch, C. Leixnering, and D. Engel, “Update: Lessons Learned from Implementing a Privacy-Preserving Smart Contract in Ethereum,” 2017-03, Nov. 2017.
[Unterweger18] A. Unterweger, F. Knirsch, C. Leixnering, and D. Engel, “Lessons Learned from Implementing a Privacy-Preserving Smart Contract in Ethereum,” in 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018.
[Venkatesh08] V. Venkatesh, H. Bala (2008), ‘Technology acceptance model 3 and a research agenda on interventions’, Decision Science 39(2), 273–315.
[Wood17a] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” 2017, Online: https://ethereum.github.io/yellowpaper/paper.pdf (accessed on August 24, 2017).
[Wood17b] G. Wood, “Polkadot: Vision for a Heterogeneous Multi-Chain Framework,” 2017, Online: https://github.com/w3f/polkadot-white-paper/raw/master/PolkaDotPaper.pdf (accessed on August 24, 2017).
[Wüst17] K. Wüst and A. Gervais, “Do you need a Blockchain,” Report 2017/375, 2017.
[Zyskind15] G. Zyskind, O. Nathan, and A. S. Pentland, “Decentralizing privacy: Using blockchain to protect personal data,” in Proceedings – 2015 IEEE Security and Privacy Workshops, SPW 2015, 2015, pp. 180–184.

7 Anhang

Alle aus dem Projekt entstandenen Publikationen sind unter folgendem Link im Volltext abrufbar:
https://www.en-trust.at/publications

8 Kontaktdaten

Dominik Engel
Zentrum für sichere Energieinformatik
Fachhochschule Salzburg
Urstein Süd 1
A-5412 Puch/Salzburg
office.zse@fh-salzburg.ac.at
+435022111300

Peter Fröhlich
Austrian Institute of Technology
Center for Technology Experience
Giefinggasse 2
1210 Wien
peter.froehlich@ait.ac.at
+43 50550-4510