Dezentralisierte Flexibilitätsplattformen

Decentralized Smart Market Design

Development of a Methodology to Identify and Evaluate Design Alternatives of a Local Flexibility Market by Application of Blockchain Technology

17.11.2021

Andreas Zeiselmair

2021

Motivation & Forschungsfragen

Motivation

Energiewende Trends: *Dekarbonisierung – Dezentralisierung – Digitalisierung – Demokratisierung*

Smart Market Plattformen schaffen einen marktbasierten Mechanismus zur netzdienlichen Nutzung kleinteiliger, dezentraler Flexibilität für das Engpassmanagement.

Blockchain bietet als Infrastruktur-Technologie manipulationsresistente Transparenz.

Forschungsfragen

RQ1: Welche *Anforderungen* an die Gestaltung einer *Smart Market Plattform* bestehen aus Sicht der beteiligten Akteure sowie energiewirtschaftlichen, technischen und marktlichen Vorgaben?

RQ2: Welche *Funktionen, Prozesse und Schnittstellen* werden in einem effizienten Smart Market Design benötigt und wie können diese technisch umgesetzt werden?

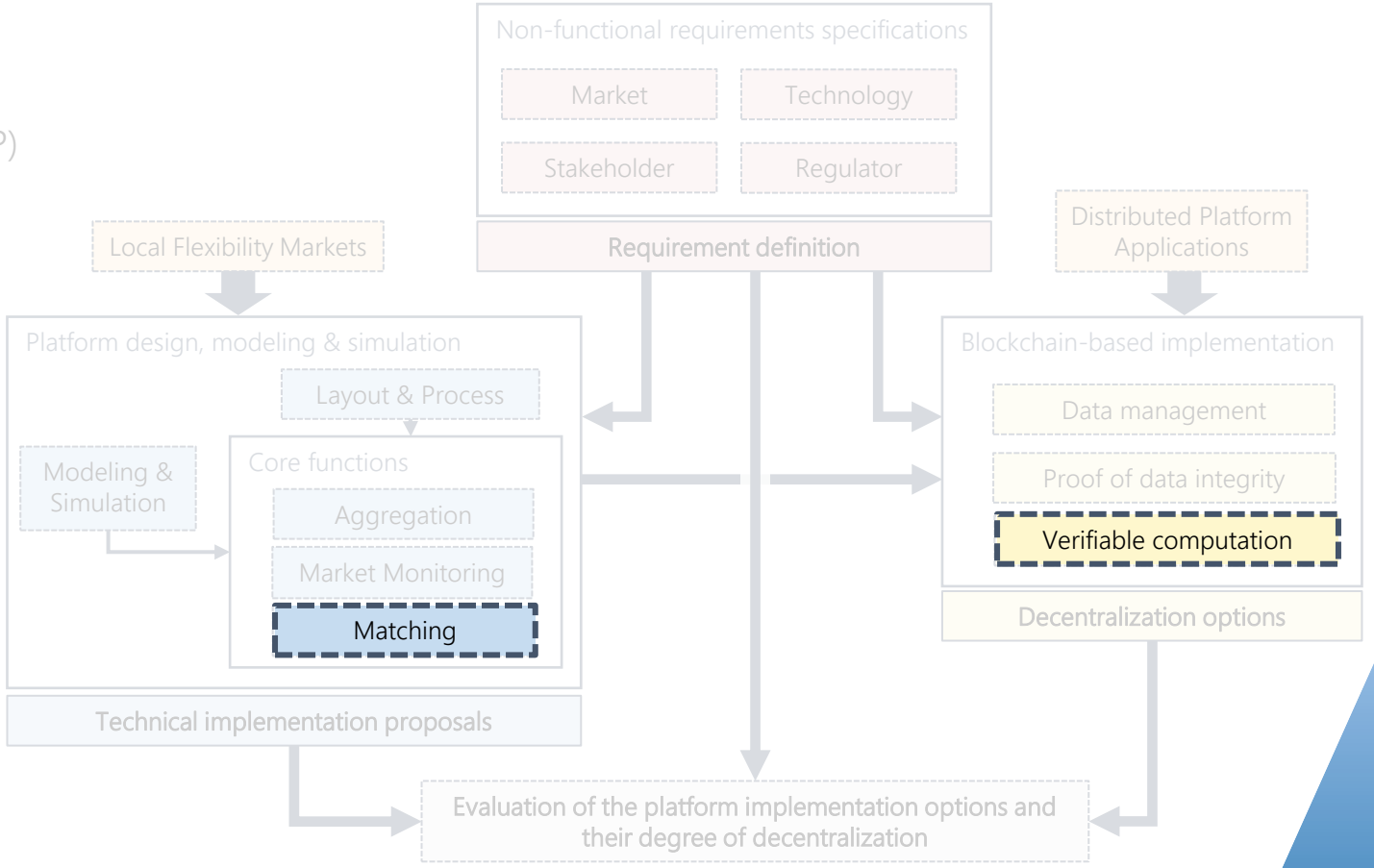
RQ3: Welche *Dezentralisierungsoptionen* bestehen und welchen Mehrwert kann die *Blockchain-Technologie* für die Umsetzung der Plattform bringen?

RQ4: Welche der ermittelten Ausgestaltungsvarianten bietet den *größten Mehrwert* im Hinblick auf die gestellten Anforderungen?

Aufbau der Arbeit

Kerninhalte

- Grundlagen und Anforderungsanalyse zur Ausgestaltung einer Smart Market Plattform (SMP)
- Funktionale SMP Ausgestaltung, Umsetzung und Simulation/Modellierung mit Fokus auf:
  - Aggregation & Pooling
  - Market Monitoring
  - Matching
- Entwicklung Blockchain-basierter Umsetzungsvarianten
  - Dezentralisierte Datenhaltung
  - Nachweis der Datenintegrität durch Merkle Proofs
  - Nachweis korrekter Berechnung durch Verifiable Computation
- Bewertung anhand Kriterienset und standardisierter Beschreibungsmethodik



Matching

Funktionale Anforderungen

- Day-ahead Prozess
- Nachfragen sollen möglichst umfassend und zu minimalen Kosten gedeckt werden
- Angebots-Gewichtung anhand standortabhängiger Effektivitätsfaktoren
- Berücksichtigung von (technischen) Randbedingungen und Beschränkungen

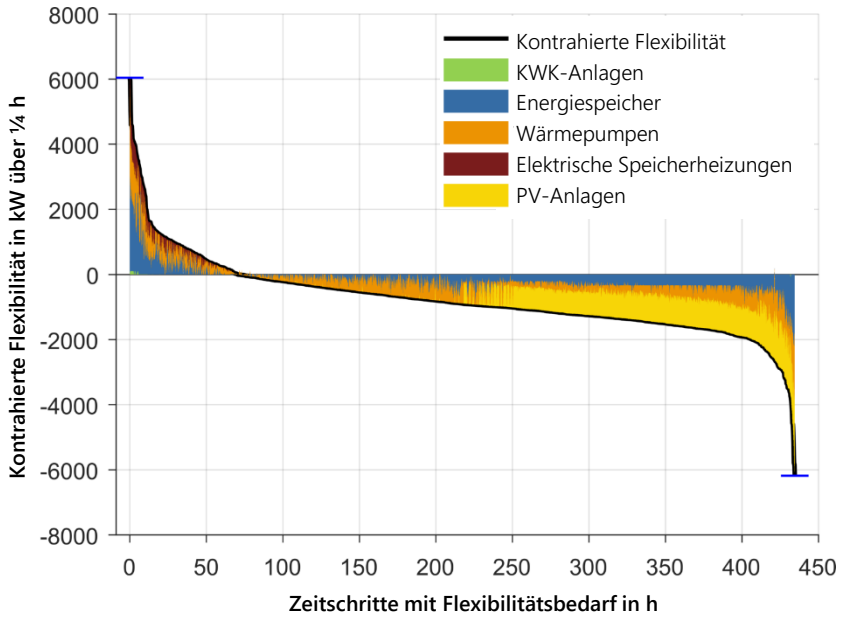
→ **Optimierungsproblem**

Implementierung: Lineare Optimierung unter Berücksichtigung von > 20 Nebenbedingungen [1]

$$\min_{P_{ij}^{+},P_{ij}^{-}} \sum_{j=1}^{96}\sum_{i=1}^{n}\left(C_{ij}^{+}\cdot P_{ij}^{+}+C_{ij}^{-}\cdot P_{ij}^{-}\right)+\sum_{l=1}^{o}G_{lj}\left(d_{jl}^{+}+d_{jl}^{-}\right)$$

Ziel: Kosten minimieren | Ziel: Nicht-Erfüllung bestrafen

Case Study: Anwendung auf ein Beispielnetz



⇨ Funktionsnachweis
⇨ Vergleich mit alternativen Ansätzen in [2]

[1] A. Zeiselmair and S. Köppl, "Constrained Optimization as the Allocation Method in Local Flexibility Markets," Energies, vol. 14, no. 13, p. 3932, Jun. 2021, doi: 10.3390/en14133932.

[2] E. Heilmann, A. Zeiselmair, and T. Estermann, "Matching supply and demand of electricity network-supportive flexibility: A case study with three comprehensible matching algorithms (in Review)." Smart Energy, 2021.

Dezentralisierte Umsetzung mittels Blockchain

Potenzieller Mehrwert für Smart Market Plattform, u.a.:

- Vermeidung eines Single-Point-of-Failure
- Transparenz für Marktteilnehmer
- Manipulationsresistenz
- Alternative Betreiberstruktur

Herausforderungen liegen v.a. in

- Datenschutz
- Skalierbarkeit
- Komplexität

→ Anwendungsbezogene Betrachtung notwendig

Verteilte Datenhaltung

→ High-level Betrachtung

Verifikation der Datenintegrität

Bewertung von alternativen Ansätzen

→ Angebots-Verifikationsverfahren inkl. PoC-Implementierung [6]

Verifiable Computation

Bewertung von alternativen Ansätzen

→ Dezentrale Optimierung im Matching inkl. prototypischer Implementierung [7]

[3] A. Zeiselmair, M. Guse, Y. Muhammad, F. Förster, G. Okwuibe, and B. Haller, "Decentralizing Smart Energy Markets - Tamper-proof Documentation of Flexibility Market Processes." Blockchain Autumn School 2020

[4] A. Zeiselmair, B. Steinkopf, U. Gallersdörfer, A. Bogensperger, and F. Matthes, "Analysis and Application of Verifiable Computation Techniques in Blockchain Systems for the Energy Sector," Frontiers in Blockchain & Renewable Energy, 2021, doi: 10.3389/fbloc.2021.725322.

Verifiable Computation

		Sicherheit	Performance	Praxistauglichkeit
Trusted Oracles	Incentive-Compatible Off-Chaining	→	↗	↑
	Trusted Execution Environments	→	↑	↗
Zero-Knowledge Proofs	zkSNARKs	↗	↘	→
Multi-Party Computation	Linear Secret Sharing	↑	→	↓

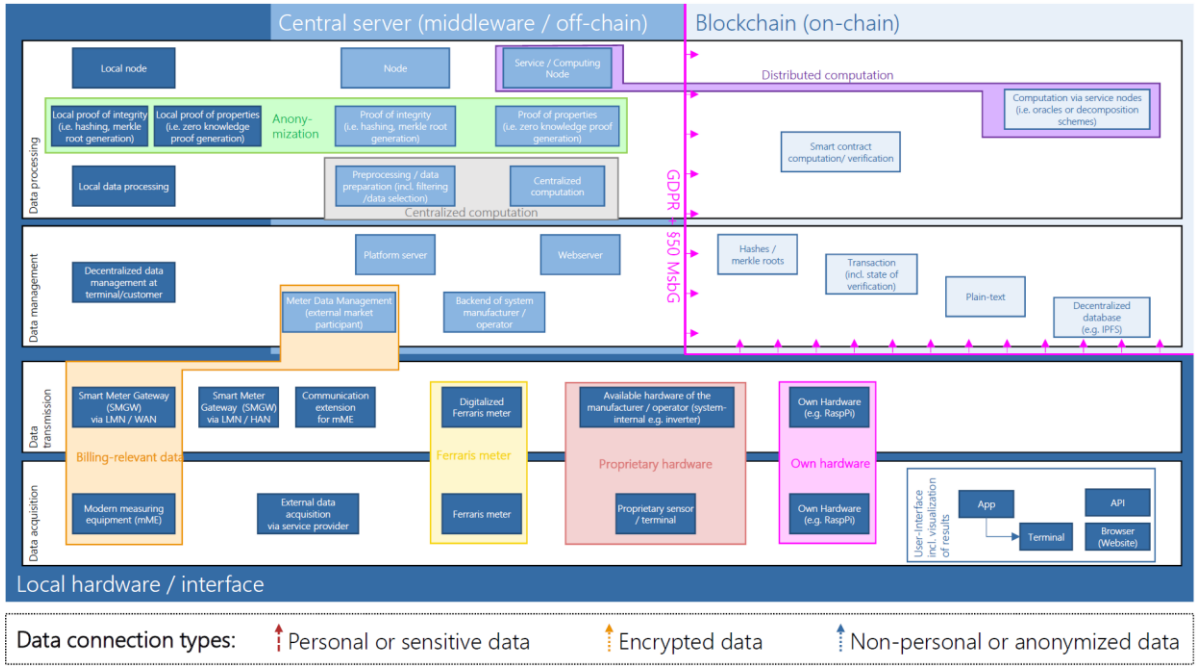
- ⇨ Verifiable Computation bietet großes Potenzial für Blockchain-basierte Energieanwendungen
- ⇨ Performance ist derzeit noch nicht ausreichend für komplexe Praxis-Anwendungen
- ⇨ Aktuell intensive Entwicklung und große Fortschritte

[4] A. Zeiselmair, B. Steinkopf, U. Gallersdörfer, A. Bogensperger, and F. Matthes, "Analysis and Application of Verifiable Computation Techniques in Blockchain Systems for the Energy Sector," Frontiers in Blockchain & Renewable Energy, 2021, doi: 10.3389/fbloc.2021.725322.

Bewertung, Fazit & Ausblick

Bewertung des Dezentralisierungspotenzials

- Standardisierter Vergleich von Designalternativen anhand entwickelter Systemarchitektur [5]
- Anwendung eines einheitlichen Kriterienkatalogs
- Anwendung von Anforderungsspezifikationen



Critical Review der Funktionen in jedem Kapitel

Fazit und Ausblick

⇨ **Umsetzungsempfehlung** anhand des Erfüllungsgrads der gestellten Anforderungen

[5] A. Zeiselmair and A. Bogensperger, "Development of a System Cartography and Evaluation Framework for Complex Energy Blockchain Architectures," ETG congress 2021.

Andreas Zeiselmair, M.Sc.

Tel.: +49(0)89 15 81 21 – 56

Email: azeiselmair@ffe.de

Vielen Dank für die Aufmerksamkeit

BACKUP

Dezentralisierte Umsetzung mittels Blockchain

Verteilte Datenhaltung

- Datenbereitstelung und –analyse
- Self-Sovereign Identity

→ High-level Betrachtung

Verifikation der Datenintegrität

Bewertung von alternativen Ansätzen

a) direkte on-chain Speicherung in Klartext
b) Ablegen eines Daten-Hashes,
c) Aggregation von Hashes mittels „Merkle tree"

→ Angebots-Verifikationsverfahren inkl. PoC-Implementierung [6]

Verifiable Computation

Bewertung von alternativen Ansätzen:

a) Trusted Oracles,
b) Zero-Knowledge Proofs,
c) Multi-Party Computation

→ Dezentrale Optimierung im Matching inkl. prototypischer Implementierung [7]

[3] A. Zeiselmair, M. Guse, Y. Muhammad, F. Förster, G. Okwuibe, and B. Haller, "Decentralizing Smart Energy Markets - Tamper-proof Documentation of Flexibility Market Processes." Blockchain Autumn School 2020

[4] A. Zeiselmair, B. Steinkopf, U. Gallersdörfer, A. Bogensperger, and F. Matthes, "Analysis and Application of Verifiable Computation Techniques in Blockchain Systems for the Energy Sector," Frontiers in Blockchain & Renewable Energy, 2021, doi: 10.3389/fbloc.2021.725322.

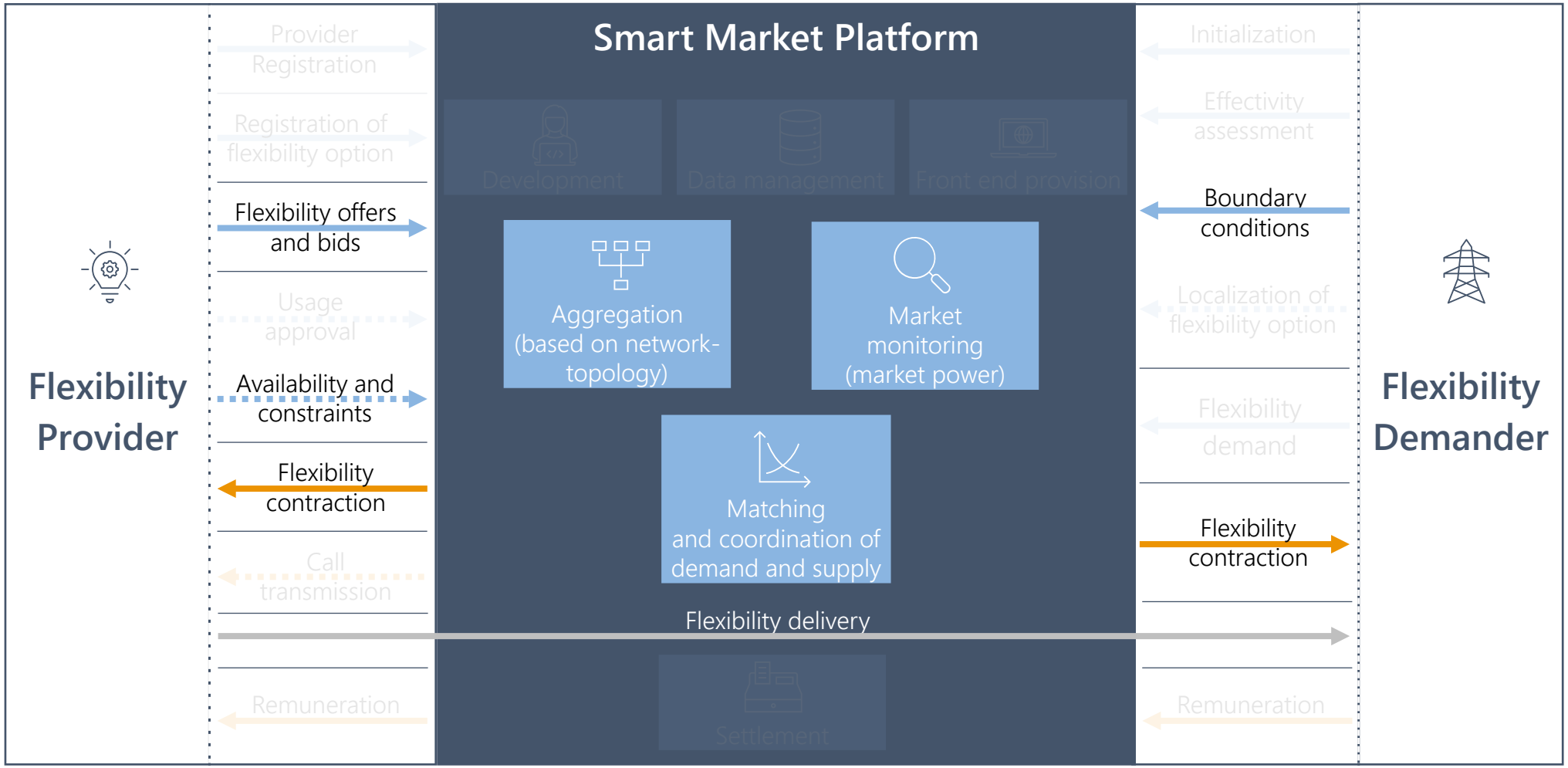
Anforderungsanalyse – “non-functional requirements”

Anforderungsanalyse

- Nicht-funktionale Anforderungen
- Input aus Projekterfahrungen und Literaturrecherche
- Grundlage für funktionale Ausgestaltung
- Basis der späteren Bewertung

		A Market perspective	B Platform participants’ perspective	C Technological perspective	D Regulatory perspective
1	**Practicality/ accessibility**	**A1** High market liquidity	**B1** Asset-specific products	**C1** Standardized market access, defined interfaces	**D1** Technology neutrality
2	**Market potential/ scalability**	**A2** Sufficient performance	**B2** Inclusion of all types of potential market participants	**C2** Little technical restrictions	**D2** Large-scale application
3	**Efficiency/ market quality**	**A3** Optimal market results, avoidance of market manipulation	**B3** Demand side: reliable delivery Supply side: maximum revenue	**C3** Consideration of technical constraints	**D3** System-optimal results, avoidance of market inconsistencies
4	**Cost**	**A4** Minimal operational costs	**B4** Minimal costs for participation	**C4** Minimal extra costs through additional functions	**D4** Minimized system costs
5	**Security**	**A5** Reliable, robust market operation	**B5** Reduction of potential points-of-failures	**C5** High availability and reliable communication	**D5** Defined responsibilities
6	**Trans-parency/ data protection**	**A6** Maximum transparency	**B6** Data privacy to protect sensitive data	**C6** Protected communication and data storage	**D6** Transparency to review market operations

Funktionaler Aufbau einer Smart Market Platform



Matching

Case Study

- Anwendung auf ein Beispielnetz
- Berechnung anhand von vier Szenarien

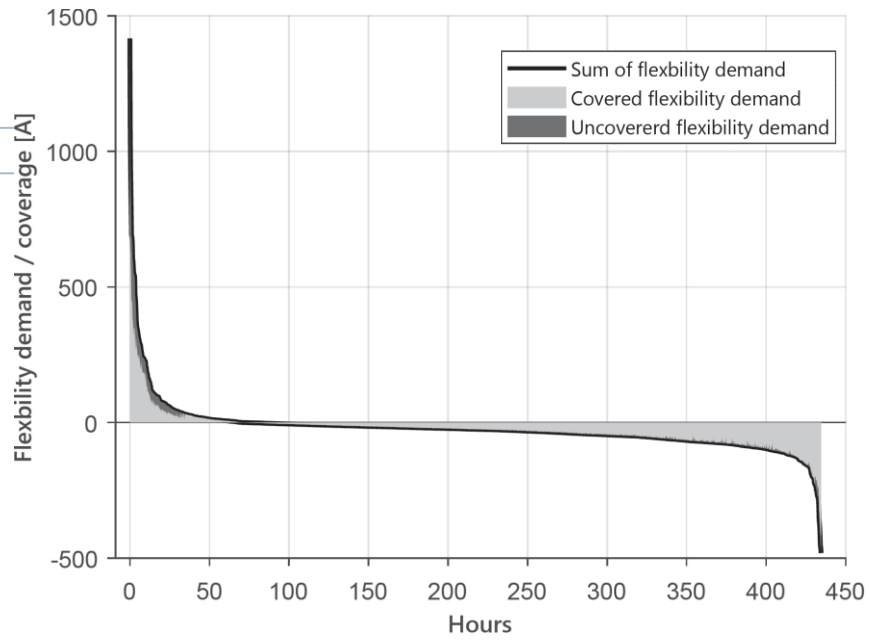
Ziel

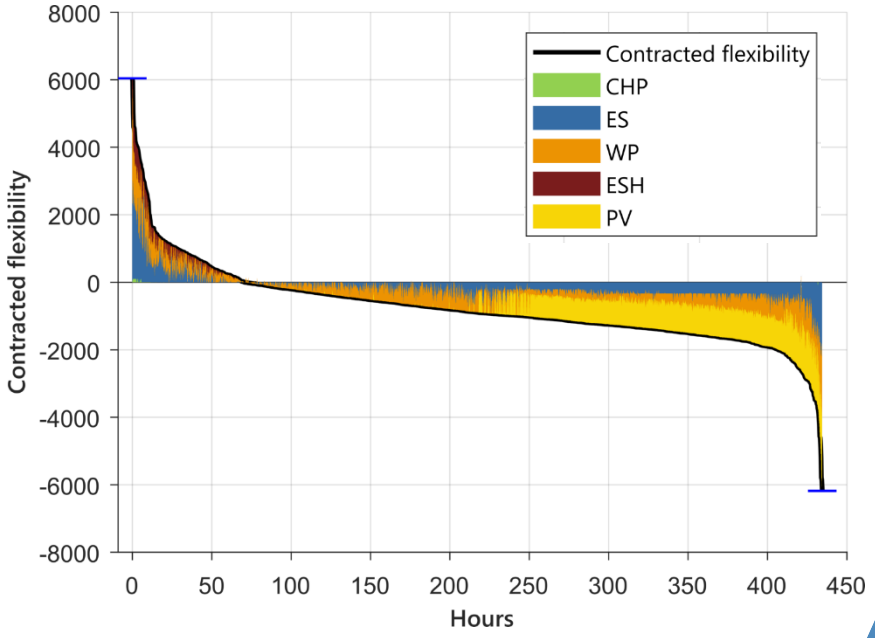
→ Nachweis der Funktionsfähigkeit

→ Analyse spezifischer Eigenschaften des Algorithmus, z. B.

- Mögliche Unter- und Überdeckung
- Einfluss des Pönalisierungsfaktors

→ Vergleich mit alternativen (heuristischen) Matching-Algorithmen [2]





[2] E. Heilmann, A. Zeiselmair, and T. Estermann, "Matching supply and demand of electricity network-supportive flexibility: A case study with three comprehensible matching algorithms (in Review)." Smart Energy, 2021.

Verifiable Computation

Blockchain-basierte Verifiable Computation

Trusted Oracles	Incentive-Compatible Off-Chaining	Ausführen von Berechnungen auf mehreren Knoten	Einzelergebnisse sammeln und zusammenführen	richtige Ergebnisse belohnen falsche Ergebnisse bestrafen
	Trusted Execution Environments	kryptografische Ko-Prozessoren sind auf CPU installiert	Erzeugung einer sicheren Laufzeitumgebung	Bescheinigung der Programmintegrität nach Abschluss
Zero-Knowledge Proofs	zkSNARKs	Übergabe von Programm *f* und Input *x*	Berechnung von $y = f(x)$ und Nachweis Erzeugung	Übergabe von y und Verifikation des Nachweises
Multi-Party Computation	Linear Secret Sharing	Aufteilung der geheimen Inputs und zufällige Verteilung	Lokale Berechnung der Anteile	Zusammenfügen der Anteile um globales Ergebnis zu erhalten

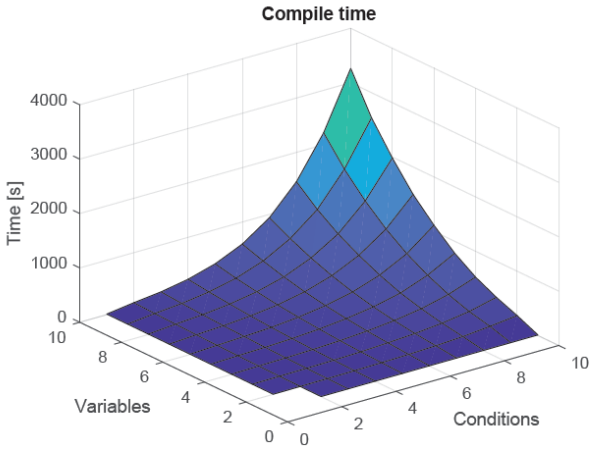
Nachweis der korrekten Berechnung mittels Verifiable Computation

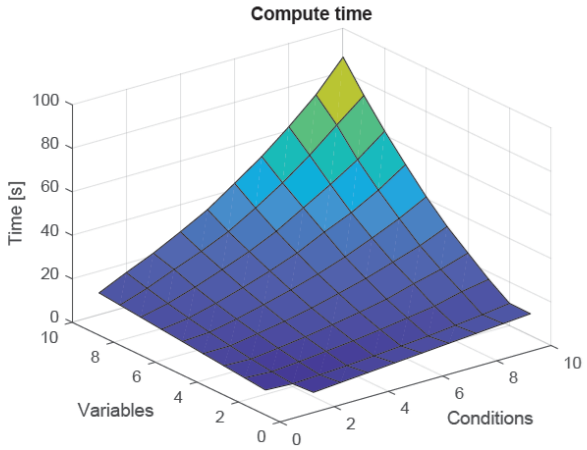
☆☆☆ Detaillierte Bewertung

	Security				Performance		Practicality		
	I	*T*	*C*	*P*	*TS*	*MC*	*M*	*U*	*E*
Trusted oracles (IOC)	-	++	--	0	0	++	++	++	++
Trusted oracles (SGX)	0	--	++	0	++	++	++	+	0
Zero-knowledge proof (Prepocessing)	+	++	0	0	0	+	0	+	-
Zero-knowledge proof (Transparent)	++	++	0	0	0	--	-	0	-
Multi-party computation (SPDZ)	++	++	++	+	--	+	-	-	-

Exemplarische Umsetzung einer linearen Optimierung mittels zkSNARKs

$$\begin{aligned} \text{maximize} \quad & c^T x \\ \text{subject to} \quad & Ax \leq b \\ \text{and} \quad & x \geq 0, \end{aligned}$$





[4] A. Zeiselmair, B. Steinkopf, U. Gallersdörfer, A. Bogensperger, and F. Matthes, "Analysis and Application of Verifiable Computation Techniques in Blockchain Systems for the Energy Sector," Frontiers in Blockchain & Renewable Energy, 2021, doi: 10.3389/fbloc.2021.725322.