B210 Decentralized Systems

Es ist schon erstaunlich. Das Internet geht auf eine Initiative aus den 1960ern zurück, ein resilientes Netzwerk aufzubauen, das buchstäblich dem Angriff einer feindlichen Macht widerstehen könne [1]. In der Gegenwart sehen wir, dass das dominierende Architekturprinzip von verteilten IT-Anwendungen das Client-Server-Prinzip ist. Das ist exakt das Prinzip, dass wir (als Community) mit dem Internet überwinden wollten. Lief dann wohl eher so mittel. Distributed Denial-of-Service (DDoS) Attacken funktionieren nur auf zentralen Systemen. Wir gehen nur am Rande der Frage nach, warum so viele Systeme auf diesen so leicht verletzbaren Prinzip basieren. Nur in Stichworten:

- Basis der Geschäftspläne (Wenn Nutzer:innendaten das eigentliche Produkt einer App sind, dann braucht man die an einer Stelle.)
- Einfachheit (zentrale App lassen sich halt enorm einfach programmieren und wer mag schon gern IT studieren? Eben. Echt schwer auch.)

Umgekehrt gilt das gleiche. Ein pur dezentrales System bietet keinen zentralen Speicher für Nutzer:innendaten und damit funktionieren die leider üblichen Geschäftsmodelle des *E-Commerce* nicht. Es gibt dezentrale Systeme; die Anzahl wächst und wir sollten uns damit beschäftigen. Cloud-Systeme können dezentral sein. Blockchain-Anwendungen sind stark diskutiert; sie erscheinen als Goldstandard verteilter Systeme, vor allem bei denen die die Grundlagen so gar nicht verstehen (wollen). In social networks werden dezentrale Alternativen zu den allseits bekannte pur zentralen populärer. Es ist schon erstaunlich, dass in solchen Systemen die alten Geschäftsmodelle dann doch funktionieren. Wie das?

Hier sollten wir aus IT-Sicht genauer hinschauen:

- Kann man noch von einer dezentralen App sprechen, wenn nur *eine* Entität *alle Peers* eines P2P Systems betreibt. Technisch: ja - aus Sicht der Anwendung?
- Man kann viele P2P System durchaus auch mit nur einem Peer betreiben. Ist das dezentral?
- Viele Blockchain-Apps (Wallet) sind keine Peers, sondern vertrauen einem Peer über das mit dem P2P System kommuniziert wird. Was ist hier dezentral?
- Das gilt auch für viele (praktisch alle) dezentralen social networks.

Wissen hilft.

In diesem Kurs werden wir uns mit den Grundlagen dezentraler Systeme beschäftigen. Teilnehmer:innen werden danach verstehen wie diese Systeme funktionieren, sie wären in der Lage solche Systeme selber zu implementieren und Schwachstellen zu identifizieren. Sie kennen die Grundlagen der Programmierung solcher Systeme, wenn sie denn eine API anbieten.

Aus IT-Sicht sind es vor allem folgende Dinge, an denen sich die Unterschiede zwischen festmachen lassen und die wir diskutieren werden:

- Datenverteilung: Wie werden Daten in einem System verteilt, dass keine zentrale Einheit hat.
- Security: Die erste Anwendung der Blockchain war die Bereitstellung eines digitalen dezentralen Geldes. Unverfälschbarkeit, Nicht-Abstreitbarkeit sind offenbar wichtige Themen.
- APIs. Technik ist das eine, deren Anwendbarkeit das andere. Gerade auf diesem Gebiet gibt es viele Anwendungen und wenige Framework mit denen man programmieren kann.

Auch in diesem Kurs folge ich strikt meinem Credo: Man versteht eine IT-Sache erst dann richtig, wenn man sie einmal programmiert hat. Wir werden daher in den Übungen ein P2P System implementieren, wahlweise eine Blockchain oder ein DHT-System; mal schauen. Ich meine damit nicht, dass wir uns z.B. Ethereum her nehmen und ein paar DApps zusammen klicken. Nein. Das ist enorm simpel, deshalb reden auch so viele so viel über P2P Systeme was leider nur manchmal nicht nur falsch ist.

Wir werden so etwas wie Ethereum (stark vereinfacht) re-implementieren. Das schafft man in einem Semester. Danach wissen Sie wirklich Bescheid. Sie müssen das nicht machen; ist ein Wahlpflichtmodul. Es ist halt schon eher die rote Pille.

Im Laufe des Kurses werden wir schauen wie sich Ihre Interessen entwickeln. Wenn sich genug finden, werde wir ein oder max zwei Themen definieren, die sie im folgende Semester im Rahmen des Projektstudiums durchführen können. Sie haben dann alle Grundlagen und können auch ein nicht triviales Projekt ablegen. Wenn Sie mögen. Und dann kann man auch sehr gern eine DApp zusammen schrauben. Denn nun wissen Sie was Sie da machen.

Einige Videos finden Sie in unserer Mediathek. Das wird ausgebaut.

Prüfungsrelevante Leistungen:

- **Semesterbegleitendes Projekt (50%)** - Sie implementieren ein P2P System und beweisen, dass es geht. Ähnlich wie in Betriebssystemen und Netzwerken: Wenn Sie das gesamte Semester kontinuierlich an dem Projekt arbeiten ist das kein Aufwand. Wenn nicht wird es ein echtes Problem.
- **Klausur (50%)** - im Prüfungszeitraum gibt es eine schriftliche Klausur.

Das folgende ist nur ein Plan. Inhalt und Reihenfolge der Themen können sich jederzeit ändern. Ich mache im laufenden Semester rechtzeitig darauf aufmerksam, welche nächsten Schritte wir tun.

#	Lehreinheit	Inhalt	Links auch zum Selbststudium	Übung
1	**Einstieg**	Was ist Dezentralität. Wir reden über das große Bild und skizzieren die Herausforderungen. Wir reden über Baran, das Internet, MANETs, Gossipprotokolle und den ganzen Rest.	[1]	Wir setzen unser Projekt auf das wir im Laufe des Semesters zu einem P2P System ausbauen. Und dann machen wir in jeder Übung weiter.
2	**DHT**	Distributed Hash Table - ein P2P Prinzip von mehreren.	[4]	

3	PKI / Enryption, PGP	Wiederholung. Ich muss sicher sein, dass Sie stabile Kenntnisse dazu haben. Wir werden damit programmieren.		Wir schauen uns an, wie wir eine PKI in unser System einbinden können.
4	Merkle-Tree	Das ist die Basis, um Blockchain, konkret Bitcoin wirklich zu verstehen. Verstehen Sie das, verstehen Sie, ob und wann ein BC sicher ist und ob und wie man die hacken kann.	[10]	
	digitale Währungen	Die Grundlagen. Es geht eigentlich nur darum, dass Sie das Double-Spending-Problem verstehen. Ich meine, wirklich verstehen. Wir wollen und werden es lösen. Theoretisch und vermutlich in unserem semesterbegleitenden Projekt.		
	Blockchain / Bitcoin	Noch ein P2P Prinzip von mehreren.	[8], [9]	
	Ethereum, Solana		[2], [3]	
	Dezentrale Online Social Network (DOSN); Mastodon und Co.)	Die basieren praktisch alle auf DHT. Was schon erstaunlich ist, weil die Technologie nun gar nicht so perfekt dafür ist, aber sie ist das einzige was wir zur Hand haben.	[7]	
	Matrix	Das dezentrale Systeme	[6]	
	ASAP/Shark			
	Synchronisation dezentraler Daten.			
	MANETs	Ein P2P Prinzip von mehreren nun auf Layer2. Mal schauen, ob das zeitlich und thematisch in den Kurs passt.		
	Ausblick (nicht klausurrelevant)	Verteile Vokabulare - verteilte Agentensysteme. Letzteres ist eine spannende Technologie, die die Entwicklung von Java inspirierte, die aber praktisch niemand mehr benutzt. Schade eigentlich. Das Problem der verteilten Vokabulare bleibt und wird gerade im Zeitalter IoT praktisch sehr relevant. Wir reden von einen Web of Things oder gar einem Semantic Web of Things.		

Literatur

[1] Paul Baran: *On Distributed Communications: 1. Introduction to Distributed Communications Networks*. Rand Corperation, 1964

[2] Solana

[3] Ethereum

[4] Petar Maymounkov and David Mazieres: Kademlia: A Peer-to-peer Information System Based on the XOR Metric

[5] Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System

[6] Matrix: Open Network for secure, decentralized communication

[7] Mastodon: Decentralized Social Network

[8] Nour El Madhoun, Ioanna Dionysiou, Emmanuel Bertin: Blockchain and Smart-Contract Technologies for Innovative Applications
(Aus dem HTW-Netz heraus ist das E-Book für Studierenden frei zugänglich.)

[9] Sami Basly: Decentralized Finance
(Aus dem HTW-Netz heraus ist das E-Book für Studierenden frei zugänglich.)

[10] Hash-Baum / Merkle-Tree

[11] US4309569A Method of providing digital signatures (inventor: Merkle, Ralph C.), published Jan, 5th1982

[12] Europäisches Parlament / Europäischer Rat: MiCAR – Markets in Crypto-Assets Regulation, June 2023

Links

https://www.freepastry.org/

https://cryptomarketcap.com/learn