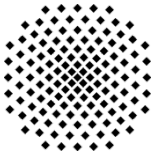


Universität Stuttgart

Institut für Parallele und Verteilte Systeme (IPVS)

Abteilung Verteilte Systeme

Prof. Rothermel

Januar 2021

Sommersemester 2021

Hauptseminar (Informatik/SWT)

Prinzipien vernetzter Systeme:

Bitcoins, Blockchains, Distributed Ledgers, … und Konsensfindung.

Bitcoins sind ein verteiltes Protokoll mit (zum aktuellen Zeitpunkt) einer Marktkapitalisierung von fast 700 Mrd. US-Dollar, Tendenz steigend. Ähnlich sieht es bei anderen, auf Blockchains aufbauenden Kryptowährungen aus. Neben ihrer Funktion am Finanzmarkt lösen diese Währungen aus technischer Perspektive das in verteilten Systemen bekannte verteilte Konsensproblem (engl. distributed consensus). Die an einer Kryptowährungstransaktion beteiligten Parteien müssen eine Einigung über den Besitzer des Geldes erzielen, da offensichtlich dasselbe Geld nicht zwei Eigentümer haben sollte. Ebenso sollte das doppeltes Ausgeben von Geld (engl. double spending) verhindert werden.

Ähnliche Konsensprobleme finden sich auch häufig in klassischen verteilten Systemen, z.B. bei der Wahl eines Master-Servers („Anführers“) aus einer Menge von redundanten Servern (Replikation von Diensten), der Orchestrierung (z.B. Apache ZooKeeper) in einem Cloud-Rechenzentrum, oder der verteilten Ausführung von Transaktionen.

Interessant sind vor allem die unterschiedlichen Methoden, mit denen das Konsensproblem gelöst wird, und die Herausforderungen, die damit einhergehen. Ein Schwerpunkt dieses Hauptseminars wird daher die Präsentation und Diskussion unterschiedlicher Blockchain-Protokolle und Kryptowährungen, wie Bitcoin, XRP („Ripple“) sowie der klassischen und insbesondere auch der neuen Methoden zur Erzielung eines Konsens sein, z.B. Proof of Work, Proof of Stake, usw.

Neben den Grundlagen von Blockchains und den verschiedenen Fragestellungen zum Konsensproblem schauen wir uns schließlich weitere Anwendungsfälle von Blockchains an, beispielsweise der Einsatz von Blockchains in Smart Contracts, zur Sicherung der Kommunikation im Internet der Dinge (IoT) und im Supply Chain Management. Ferner werden alternative „Distributed-Ledger“-Systems, und darüberhinausgehende verteilte Systeme mit ähnlichen Problemstellungen diskutiert.

Voraussetzungen: Grundkenntnisse in Verteilten Systemen sind hilfreich (die Vorlesung Verteilte Systeme ist aber nicht zwingend erforderlich).

Weitere Informationen werden nach der Registrierung über ILIAS bekanntgegeben.

Sprache: Deutsch. Vorträge und Ausarbeitungen dürfen auch auf Englisch gehalten bzw. verfasst werden.

Kontakt:

Kurt Rothermel (Prüfer) (kurt.rothermel@ipvs.uni-stuttgart.de)
Jonathan Falk (jonathan.falk@ipvs.uni-stuttgart.de)
Henriette Röger (henriette.roeger@ipvs.uni-stuttgart.de)