Blockchain Business Development

Decentralized Systems

CBS, DIKU

Copenhagen, Denmark

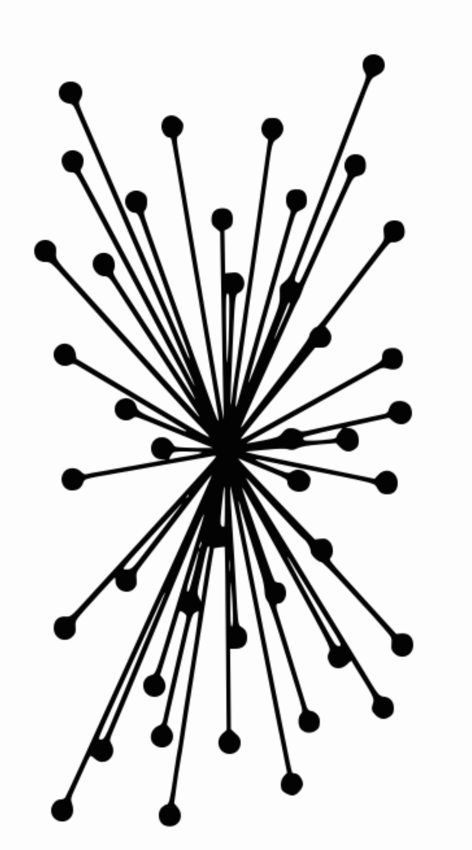
9/9/2020

Boris Düdder

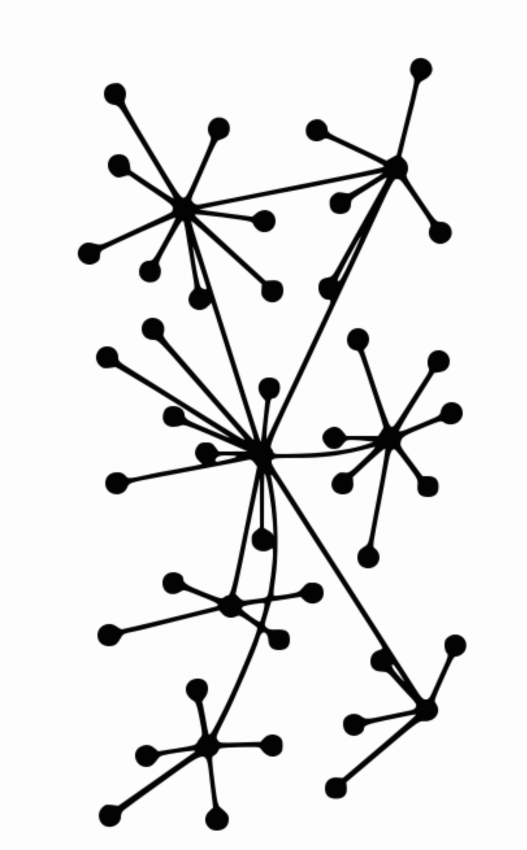
UNIVERSITY OF COPENHAGEN

Distributed is not decentralized

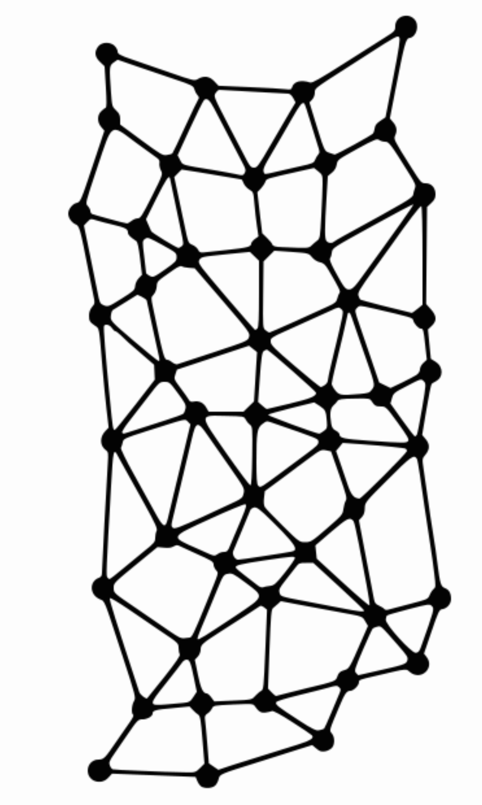
Centralized



Hierarchical



Distributed and decentralized



Network of …

- **Computers**, each running a specific program
- **Connections** for sending and receiving data

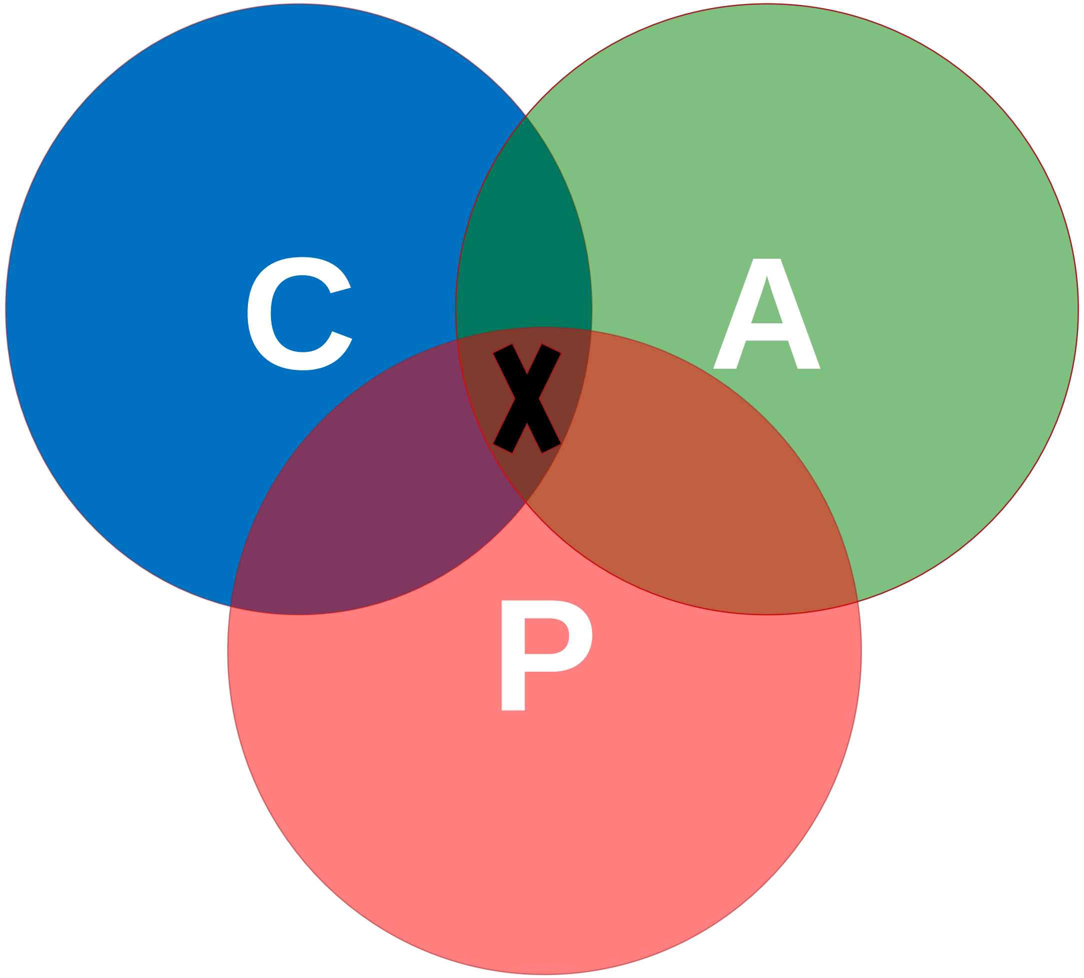
… which collectively offers

- A coherent **interface** to client computers

Distributed systems can have 3 very attractive properties

Properties	What does it mean?	Why do we care?
Consistency	Clients get same response, independent of node accessed	We don't want different answers to the same question!
Availability	All clients get a response eventually (fast enough)	We need an answer sooner than later!
Partition tolerance	All accessible nodes respond, even when internal communication is impossible (slow)	The system works even in off-line mode (not net or slow net)

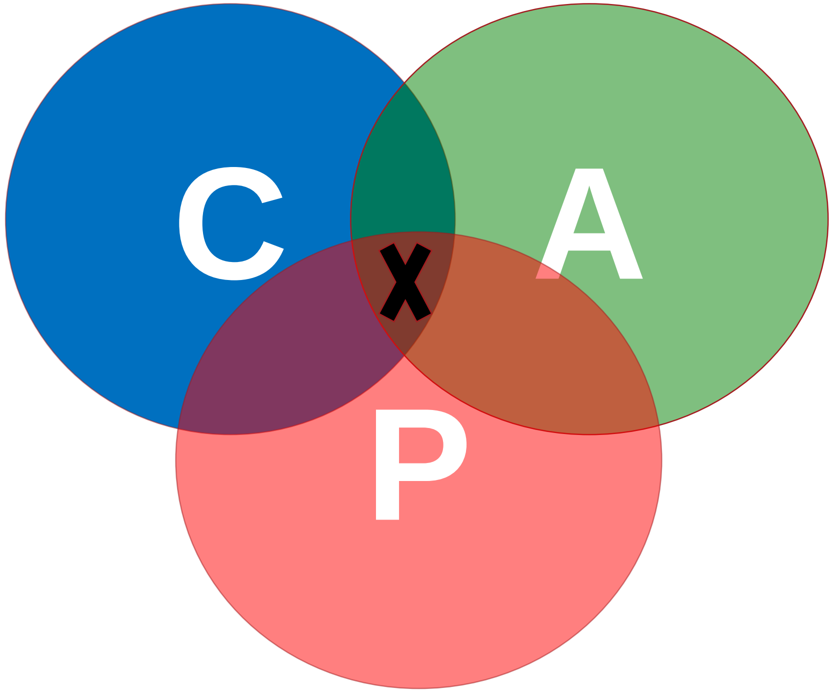
CAP Theorem



Conjecture by Eric Brewer at Symposium on Principles of Distributed Computing (PODC), 2000

Revisit CAP Theorem

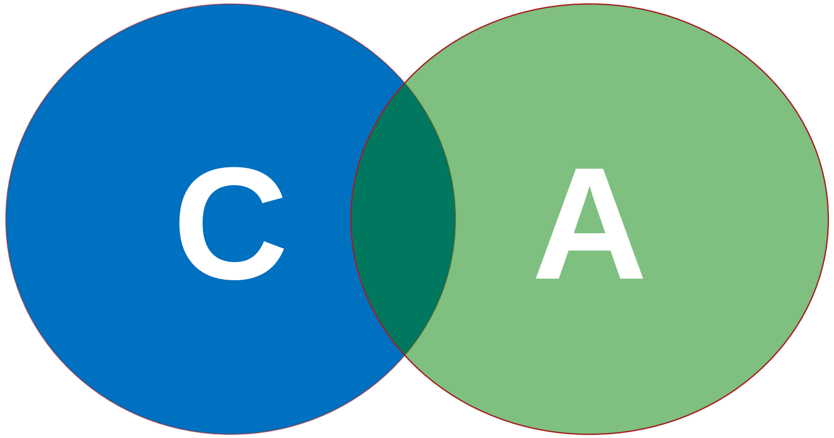
- Of the following three guarantees potentially offered a by distributed systems:
  - **Consistency**
  - **Availability**
  - **Partition tolerance**



- This suggests there are **three** kinds of distributed systems:
  - CP, AP, CA

A popular misconception: 2 out 3

- How about **CA**?
- Can a **distributed** system (with unreliable network) really be **not** tolerant of partitions?
- Pick out of **two**



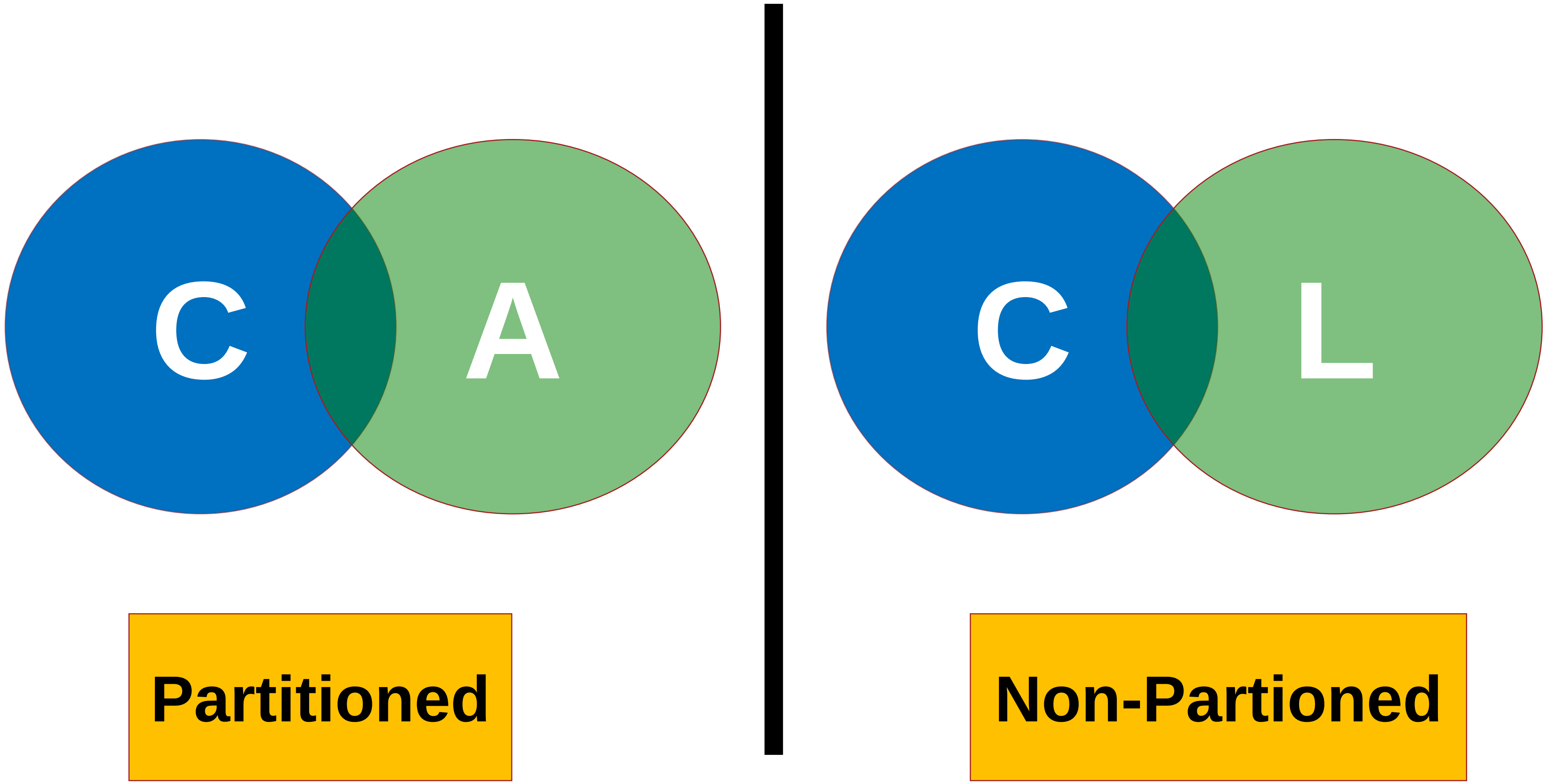
CAP → PACELC

A more complete description of the space of potential **trade-offs** for distributed system:

- **If** there is a **partition (P)**, how does the system trade off availability and consistency (**A and C**);
- **else (E)**, when the system is running normally in the absence of partitions, how does the system trade off latency **(L) and** consistency **(C)**?

Abadi, Daniel J. "Consistency trade-offs in modern distributed database system design." Computer-IEEE Computer Magazine 45.2 (2012): 37-42.

PACELC



Consensus algorithms

Consensus algorithms allow **collection of machines** to work as **coherent group** that can **survive failures** of some of its members and remain consistent

Very important role in building **fault-tolerant** distributed systems

Safety: **Never return incorrect result** under all kinds of non-Byzantine failures

Availability: **Remain available** as long as **majority** of servers remain operational and can communicate with each other and with clients

[Dwork et al. 1988] Consensus under Presence of Partial Synchronicity

TABLE I. SMALLEST NUMBER OF PROCESSORS N_{min} FOR WHICH A t-RESILIENT CONSENSUS PROTOCOL EXISTS

Failure type	Synchronous	Asynchronous	Partially synchronous communication and synchronous processors	Partially synchronous communication and processors	Partially synchronous processors and synchronous communication
Fail-stop	t	∞	$2t + 1$	$2t + 1$	t
Omission	t	∞	$2t + 1$	$2t + 1$	$[2t, 2t + 1]$
Authenticated Byzantine	t	∞	$3t + 1$	$3t + 1$	$2t + 1$
Byzantine	$3t + 1$	∞	$3t + 1$	$3t + 1$	$3t + 1$

Source: Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer. 1988. Consensus in the presence of partial synchrony. J. ACM 35, 2 (April 1988), 288-323. DOI=http://dx.doi.org/10.1145/42282.42283

[Blockbench17] Performance Scalability

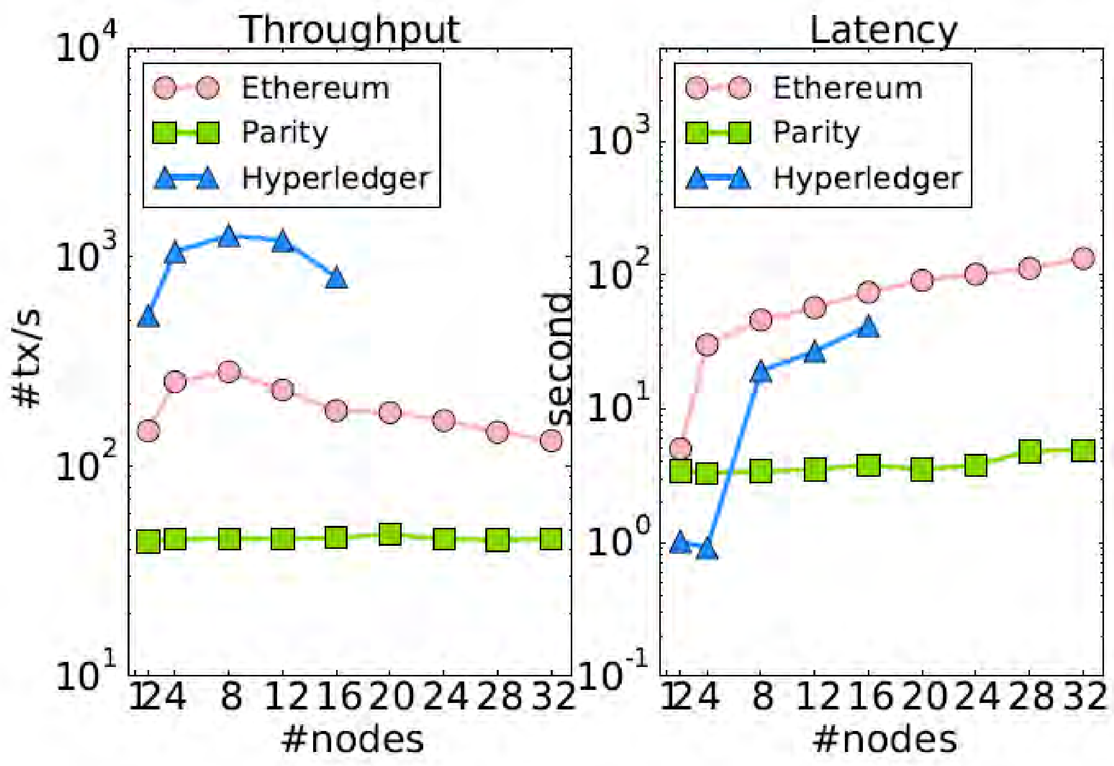


Figure 7: Performance scalability (with the same number of clients and servers).

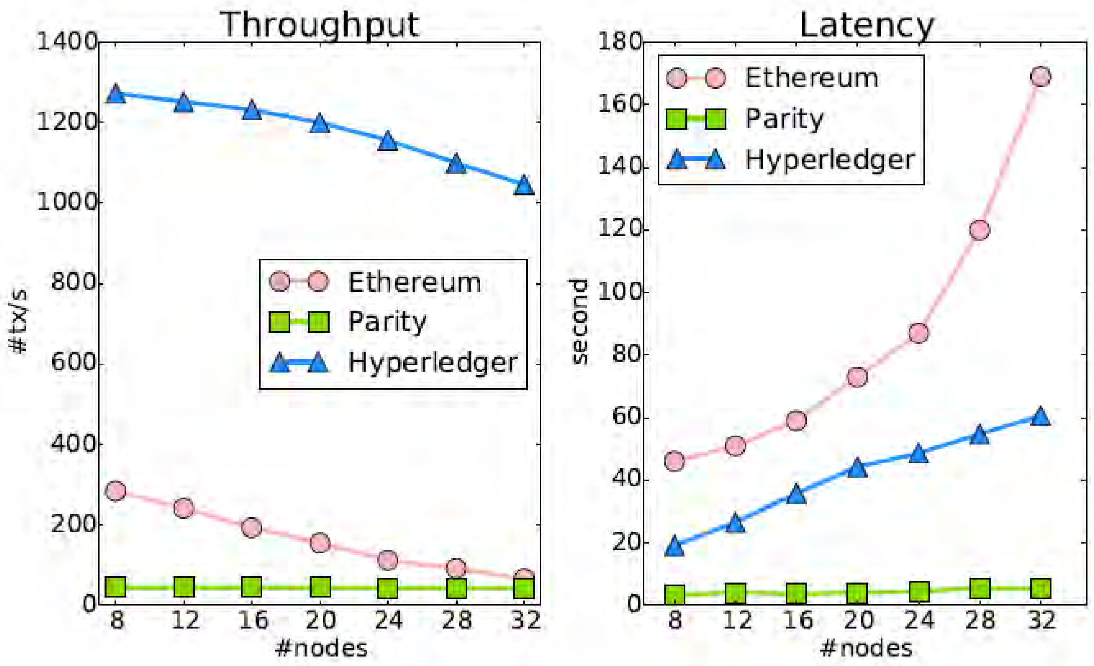
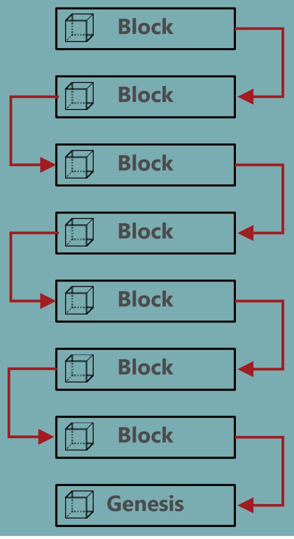


Figure 8: Performance scalability (with 8 clients).

How do we verify a state and generate consensus in a blockchain / DLT?



Proof-of-Work (PoW)

Energy as evidence for consent behavior

Dwork & Naor 1993, Jakobsson & Juels 1999

Proof-of-Stake (PoS)

Economic value as evidence for consent behavior

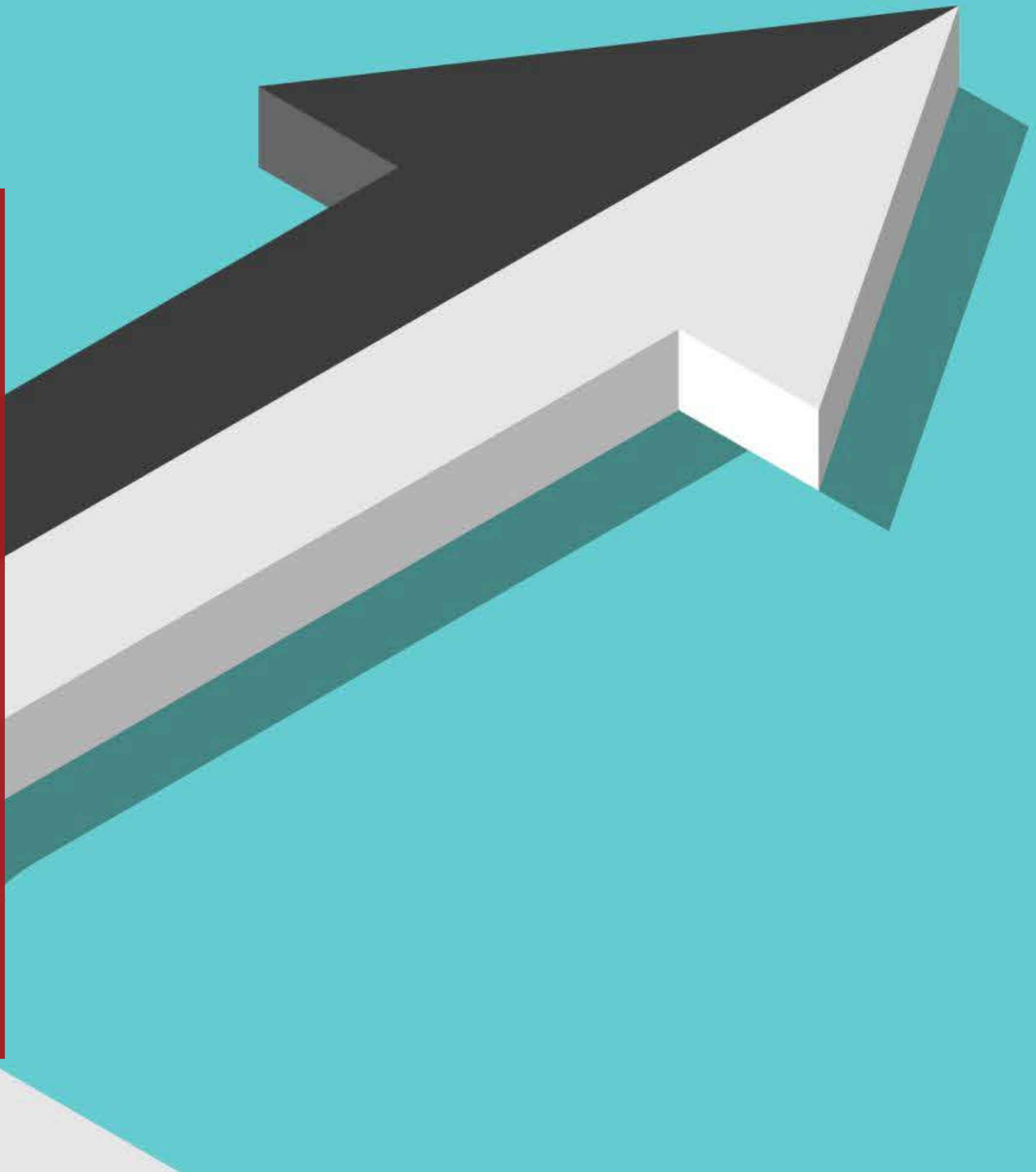
Kiayias et al. 2017

Proof-Of-Location (PoL)

Physical locality as evidence for consent behavior (IIoT)

Dasu et al. 2018

- Decentralized system is special for of distributed system
- CAP Theorem has impact on distributed systems
- Impact on performance depending on used protocols



Next lecture on

Cryptography

9/9/2020 at 12:35-16:05 online