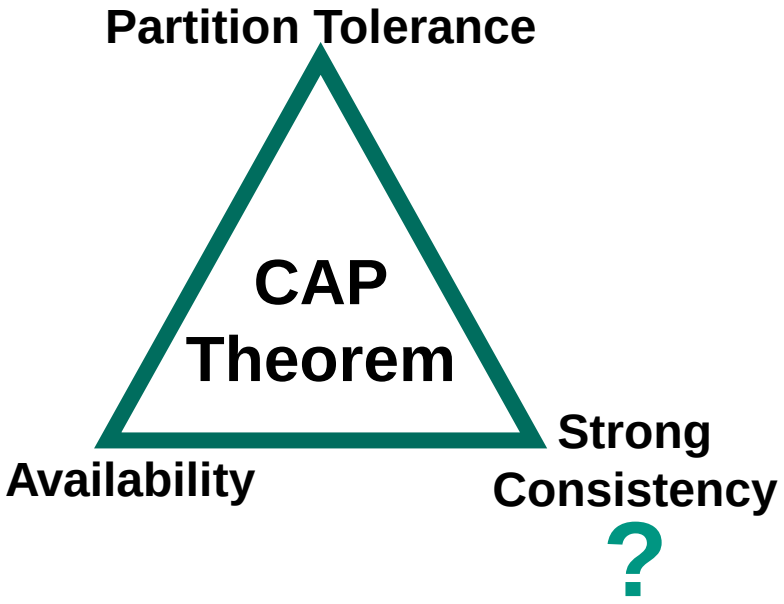
Karlsruhe Institute of Technology

Weakly Consistent but Eventually Convergent: Access Control in the Matrix Messaging System

Florian Jacob, Hannes Hartenstein

Lightning Talk @ SACMAT 2023

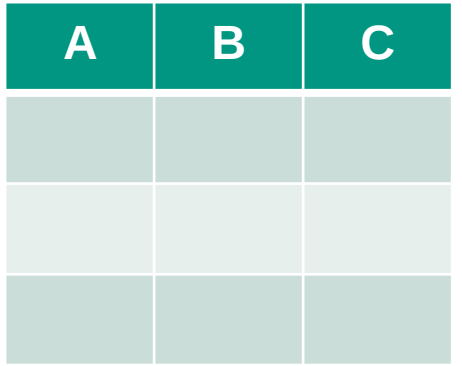
[matrix]



Centralized Applications and Access Control

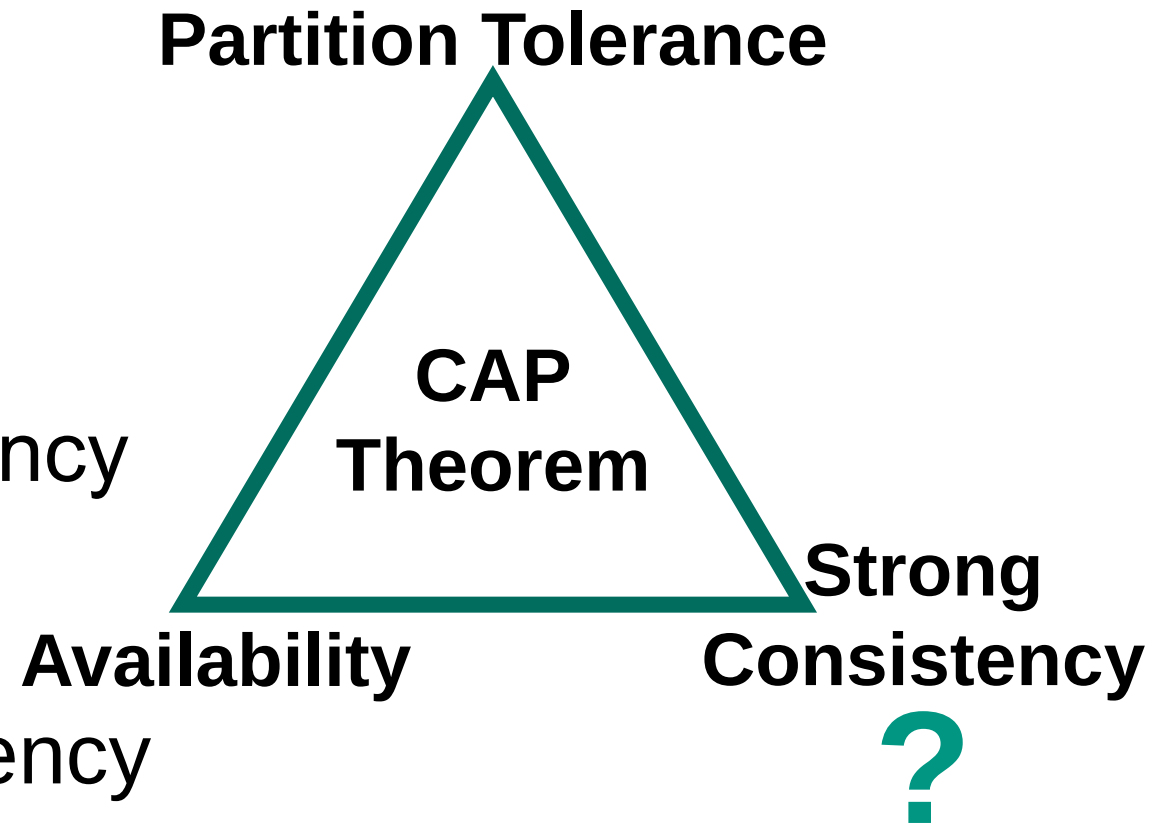
- A single logical entity…
  - …executes the application
  - …defines a total order on incoming access requests
  - …knows all current policies & permission assignments
  - …decides and enforces policies

- Centralization is a standard assumption
  - Example: Scot Stoller's keynote "WebSheets: A Framework for Privacy-Centric Web Applications by Non-Programmers"



Problem: Distributing Apps and Access Control

- One wants to make an application distributed to get…
  - Scalability
  - Low Latency
  - Availability
  - Fault Tolerance
- …while keeping Strong Consistency
  - “Behave as if still centralized!“



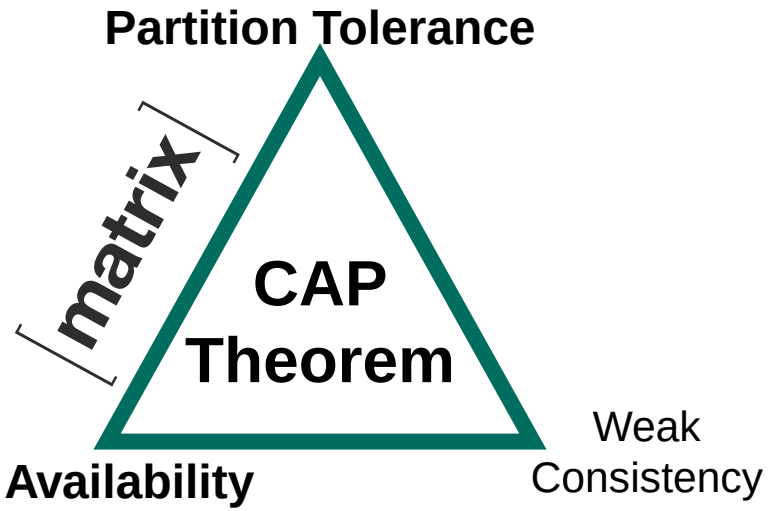
- ▶ Everyone wants Strong Consistency
  - ▶ but no one wants to pay its price!

Does Matrix have a Solution?

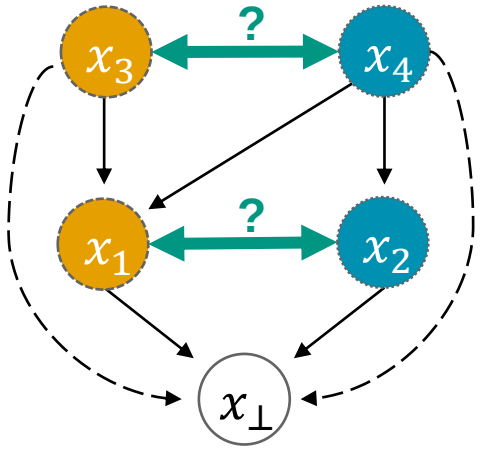
- Matrix is a relevant decentralized messaging middleware
  - $\gtrapprox 100\,000\,000$ accounts, $\gtrapprox 100\,000$ servers
  - Universities, Mozilla Foundation, French and German Public Sector, …
- Matrix provides access control in an unconventional environment
  - weakly consistent, no consensus
  - servers independently decide
  - …but decisions still eventually converge.

matrix

element.io



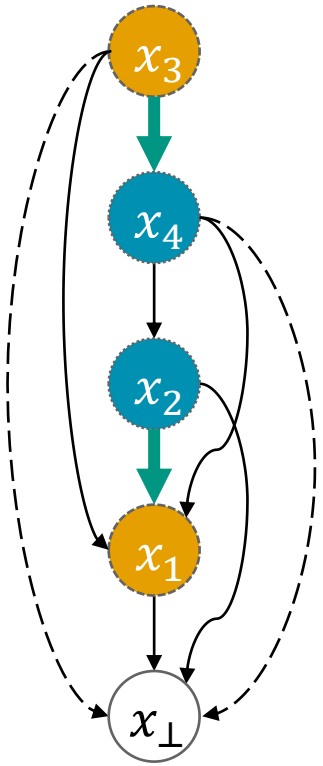
Replicated Building Blocks: Sets and Maps



Extend partial to linear order:

$x_3 \| x_4 ?\ h(x_3) < h(x_4) \Rightarrow x_3 < x_4$

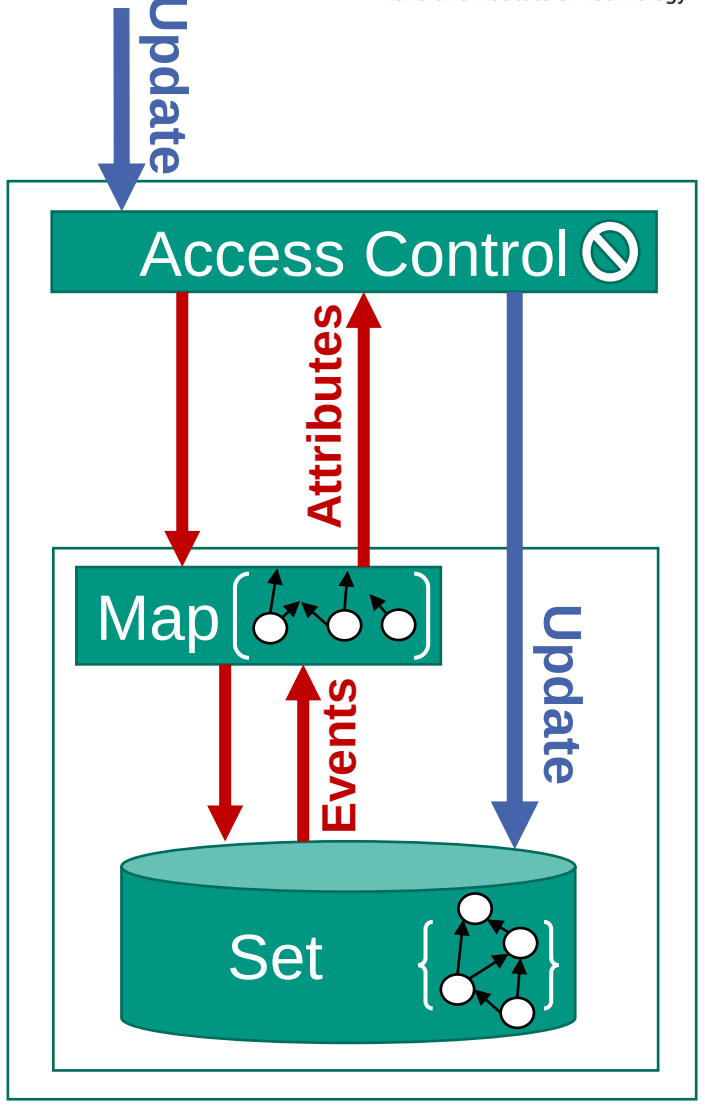
$x_1 \| x_2 ?\ h(x_1) < h(x_2) \Rightarrow x_1 < x_2$



- 1st building block: partially-ordered sets of events
  - Authorized accesses in partially-ordered time
- 2nd building block: derived key-value maps
  - Policy information attributes

Matrix' Approach to Distributed Access Control

- Decentralized access control in partially-ordered time is challenging
- Matrix' approach: compose weakly-consistent, replicated Sets and Maps to get a form of lattice-based access control
  - Never reject authorized concurrent updates
  - …but maybe collectively ignore them after linearization
  - **But: What does it mean to have "eventually convergent access control"?**



Future Work

Access Control
"Matrix Decomposition – Analysis of an Access Control Approach on Transaction-based DAGs without Finality", SACMAT 2020, doi:10.1145/3381991.3395399

Consistency
"On Extend-Only Directed Posets and Derived Byzantine-Tolerant Replicated Data Types", PaPoC 2023, doi:10.1145/3578358.3591333

Achievable strength of access control in distributed, weakly-consistent systems?

- Supported invariants and semantics
- Expected quirks and anomalies