Replicated State Machines

Q: How do we build fault tolerant services?
   -> What types of fault
   -> How severe?
     -> What types of service?
     -> What correctness guarantees?
     -> Where will the service run? What assumptions can we make?

Failure Models (What type of failure)
Fail-Stop \hspace{1cm} \rightarrow \hspace{1cm} \text{Byzantine}

\# of faulty nodes \uparrow \text{Quorum}

Asynchronous? [What will the service run?]

\text{FLP}

Partial Synchrony?

\Delta \text{message delay} \hspace{1cm} \Delta t

Clock Synchronization?
State Machines [What types of services]

Deterministic

A program whose state depends on seq. of commands

Behavior

Deterministic behavior

State Machine Replication
Dealing with I/O

State Machine Replication

Agreement + Ordering → Agreement
Logical Construction

Clients

A

B

C

D

Terminate:

Physical Challenges

Validiy?
PHYSICAL REQUIREMENTS

\[ \rightarrow \text{SEQUENCER FAULT TOLERANCE} \]

\[ \rightarrow \text{QUORUMS} \]
Replicated logs: Our Abstraction

Looking Ahead...
$R^2$

Quotient Intersection

$n$ machines

$k - n$

$\mathbb{R}$