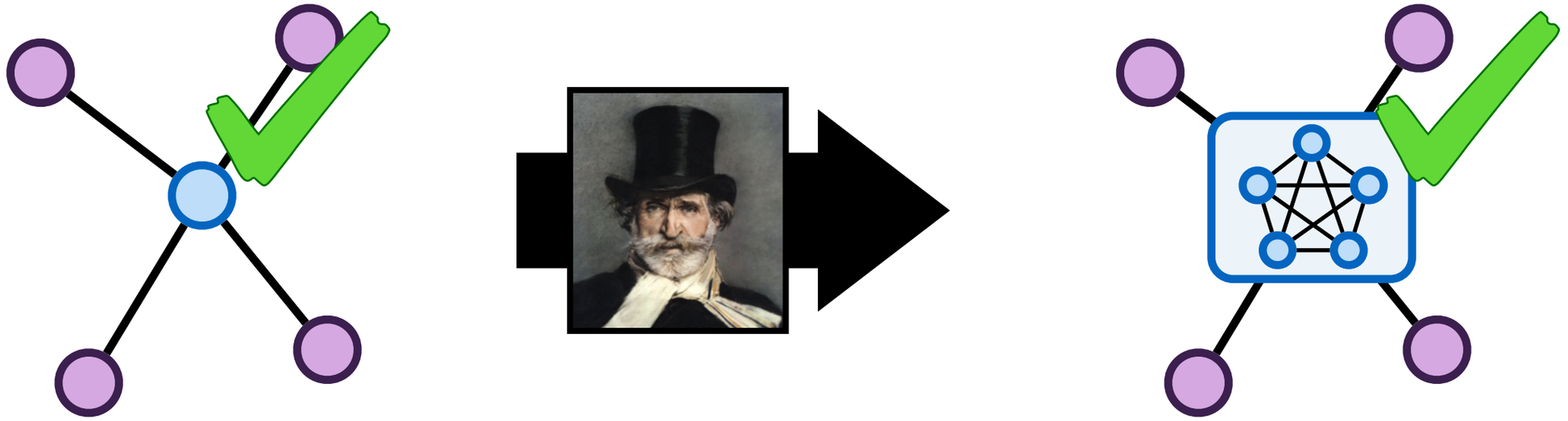
Verifying Distributed Systems



Zachary Tatlock

Verdi Lecture 1 at DeepSpec Summer School 2018

PAUL G. ALLEN SCHOOL
OF COMPUTER SCIENCE & ENGINEERING

PLSE

Verdi Team

James Wilcox

Doug Woos

Pavel Panchekha

Ryan Doenges

Justin Adsuara

Keith Simmons

Steve Anton

Miranda Edwards

Karl Palmskog

Ilya Sergey

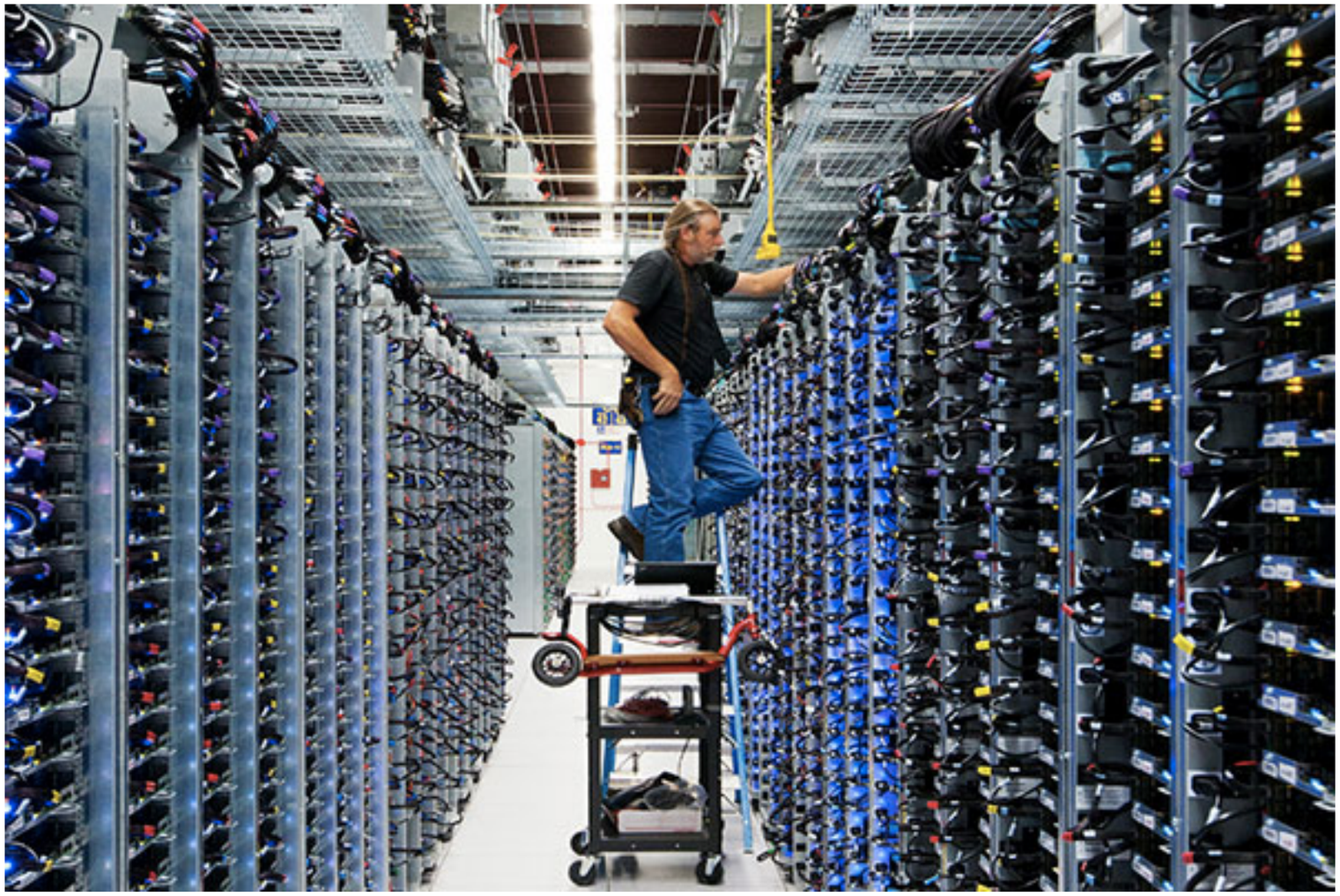
Xi Wang

Mike Ernst

Tom Anderson

Distributed Systems

Distributed Systems



Distributed Apps

Distributed Infrastructure

One summer day...

One summer day...

The New York Times

The Stock Market Bell Rings, Computers Fail, Wall Street Cringes

By NATHANIEL POPPER JULY 8, 2015

Problems with technology have at times roiled global financial markets, but the 223-year-old New York Stock Exchange has held itself up as an oasis of humans ready to step in when the computers go haywire.

On Wednesday, however, those working on the trading floor were left helpless when the computer systems at the exchange went down for nearly four hours in the middle of the day, bringing an icon of capitalism's ceaseless energy to a costly halt.

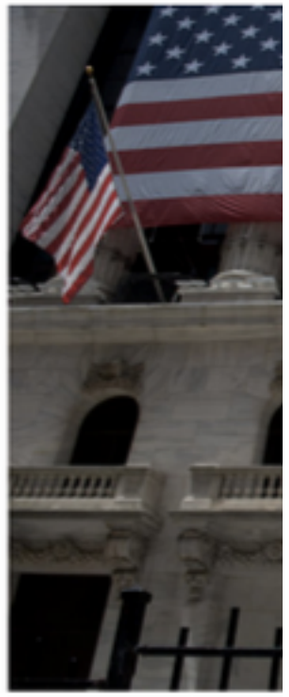
The exchange ultimately returned to action shortly before the closing bell,

One summer day...

The New York Times

The Stock Market Bell Rings, Compu

By NATHANIEL POPPER JULY 8, 2015



Problems with technology have at times roiled global financial markets, but the 223-year-old New York Stock Exchange has held itself up as an oasis of humans ready to step in when the computers go haywire.

On Wednesday, however, those working on the trading floor were left helpless when the computer systems at the exchange went down for nearly four hours in the middle of the day, bringing an icon of capitalism's ceaseless energy to a costly halt.

The exchange ultimately returned to action shortly before the closing bell,

THE WALL STREET JOURNAL. Digital Network | WSJ.com | MarketWatch | BARRON'S

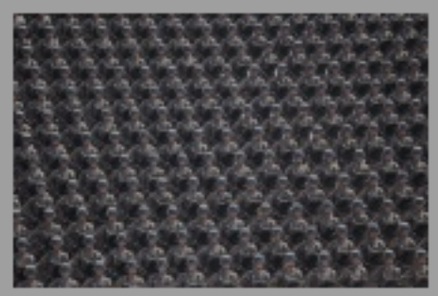
THE WALL STREET JOURNAL.

Home

WSJ.com is having technical difficulties. The full site will return shortly.

Cyber Sleuths Trac to China's Military

The story of a Chinese military staffer's ent in hacking provides a detailed look into B state-controlled cyberespionage machinery.



Debt Relief for Students Snarls Market for Their Loans

Federal programs designed to ease the burden of college loans are causing snarls in the bond market and raising concerns that banks may soon ratchet back lending.

The New Bond Market: Algorithms Trump Humans

Computerized trading strategies, or algorithms, are remaking the $12.7 trillion Treasury market, emulating earlier sea changes in stock and currency trading.

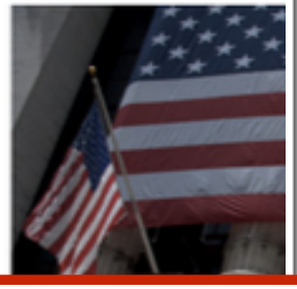
One summer day...

The New York Times

The Stock Market Bell Rings, Compu

By NATHANIEL POPPER JULY 8, 2015

Problems with technology have at times roiled global financial markets, but the 223-year-old New York Stock Exchange has held itself up as an oasis of humans ready to step in when the computers go haywire.



On Wedne
working o
helpless w
the exchar
four hours
bringing a
ceaseless

The excha
action sho

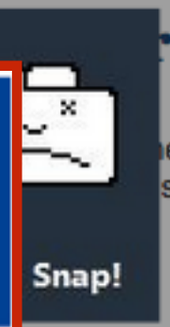
THE WALL STREET JOURNAL.
Digital Network
WSJ.com MarketWatch BARRON'S

THE WALL STREET JOURNAL.

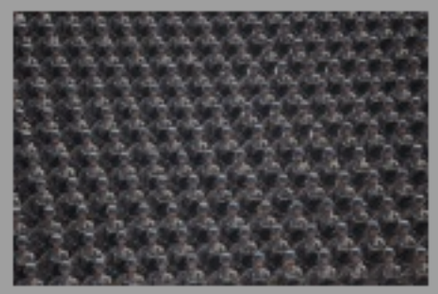
Home

WSJ.com is having technical difficulties. The full site will return shortly.

Cyber Sleuths Trac r to



ent in
state-



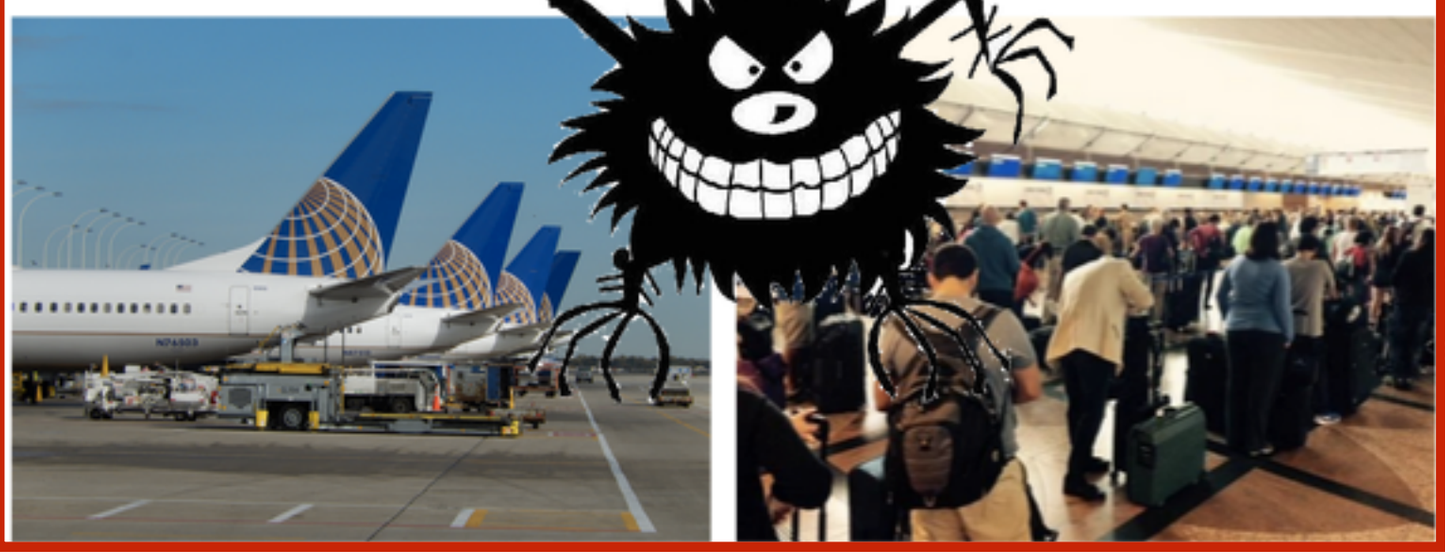
arket for Their Loans

n of college loans are causing snarls
anks may soon ratchet back lending.

s Trump Humans

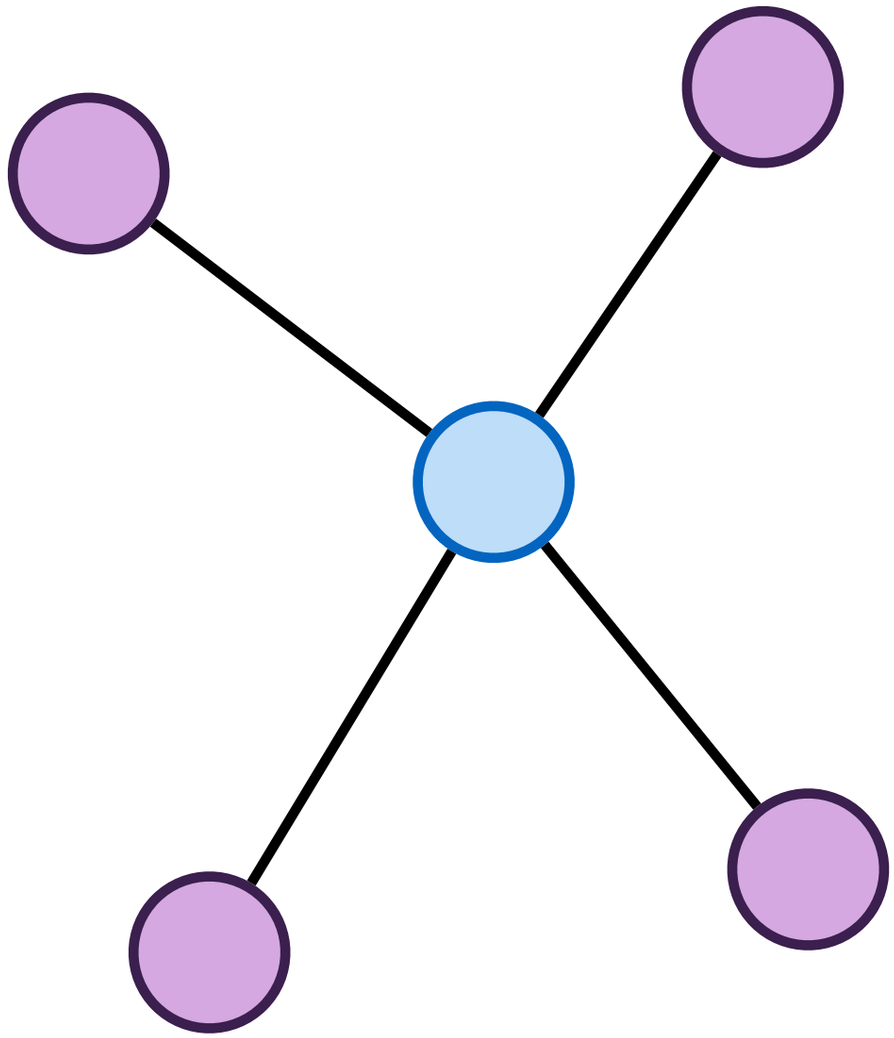
, are remaking the $12.7 trillion
s in stock and currency trading.

UNITED



How distributed systems fail

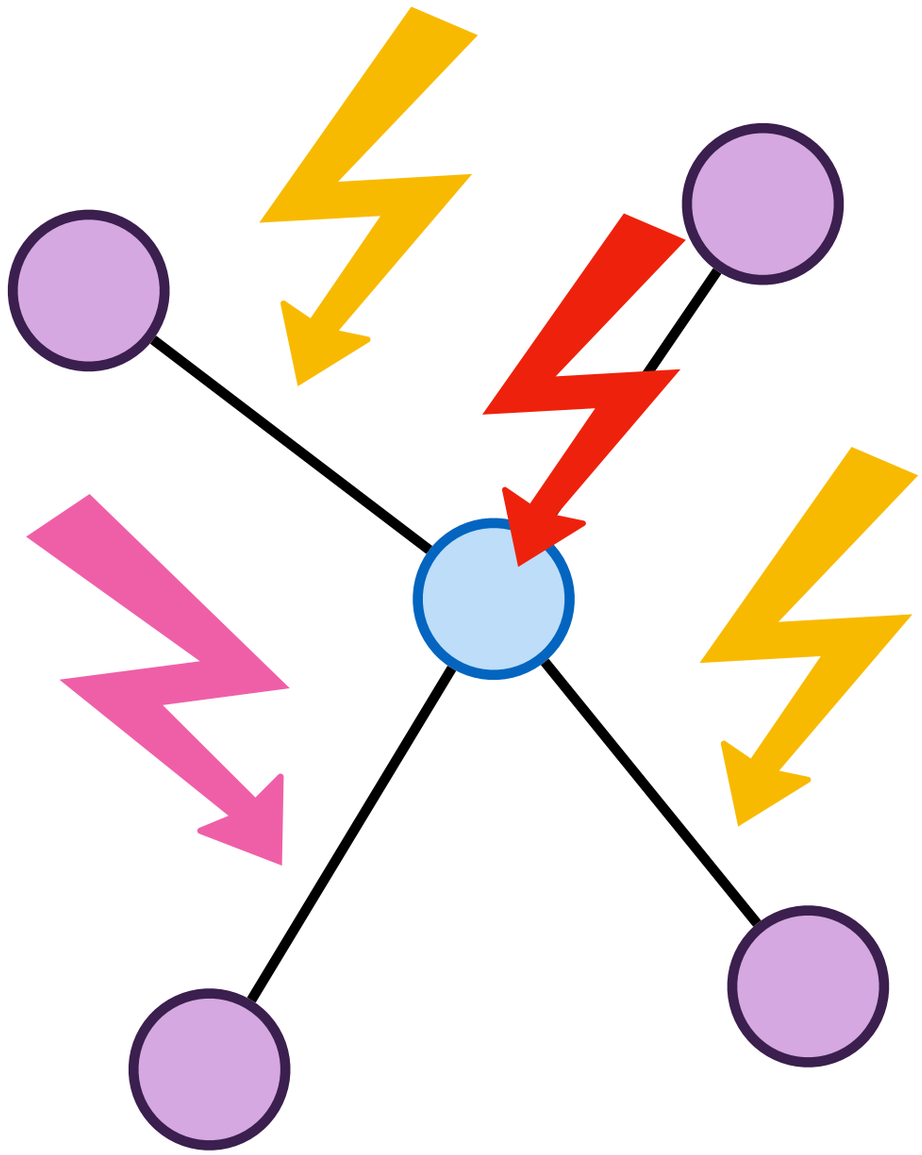
How distributed systems fail



Challenges

concurrency

How distributed systems fail



Challenges

concurrency

message drops

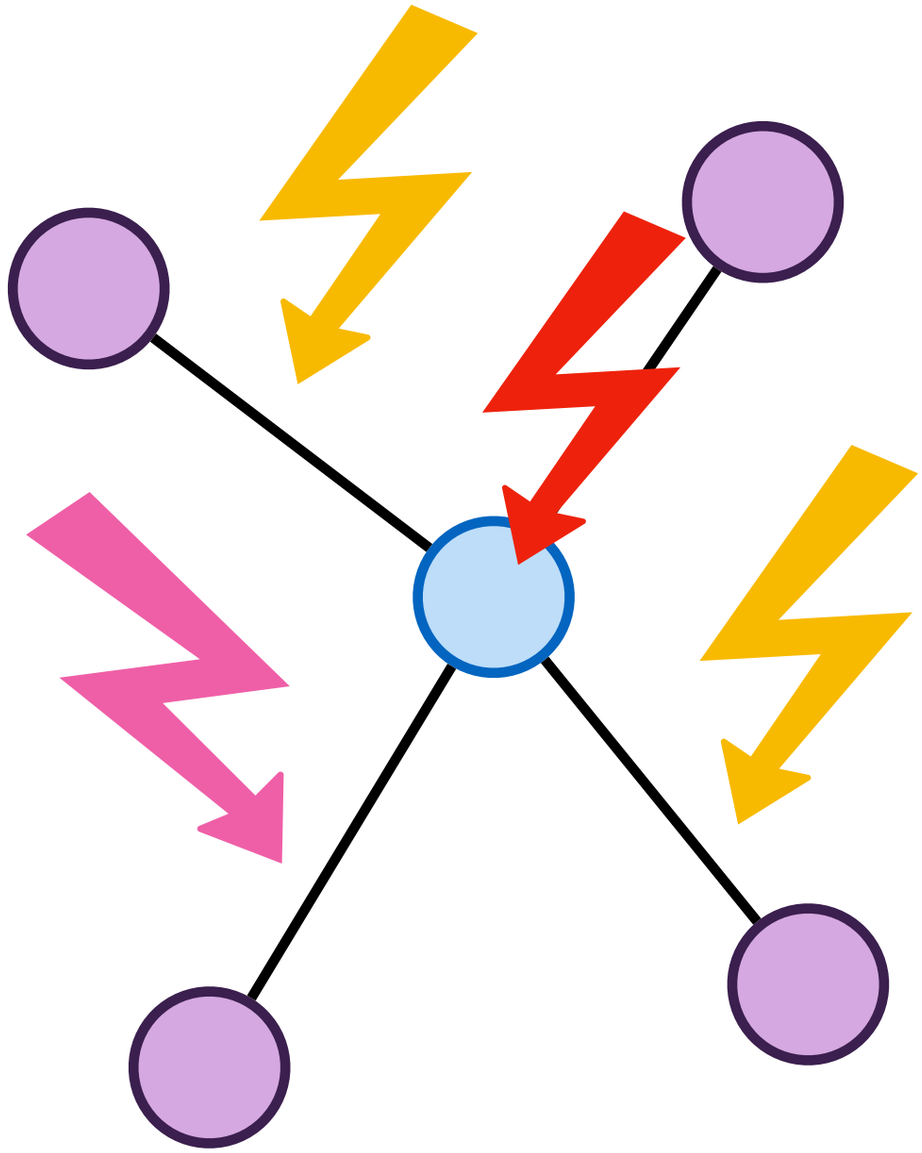
message dups

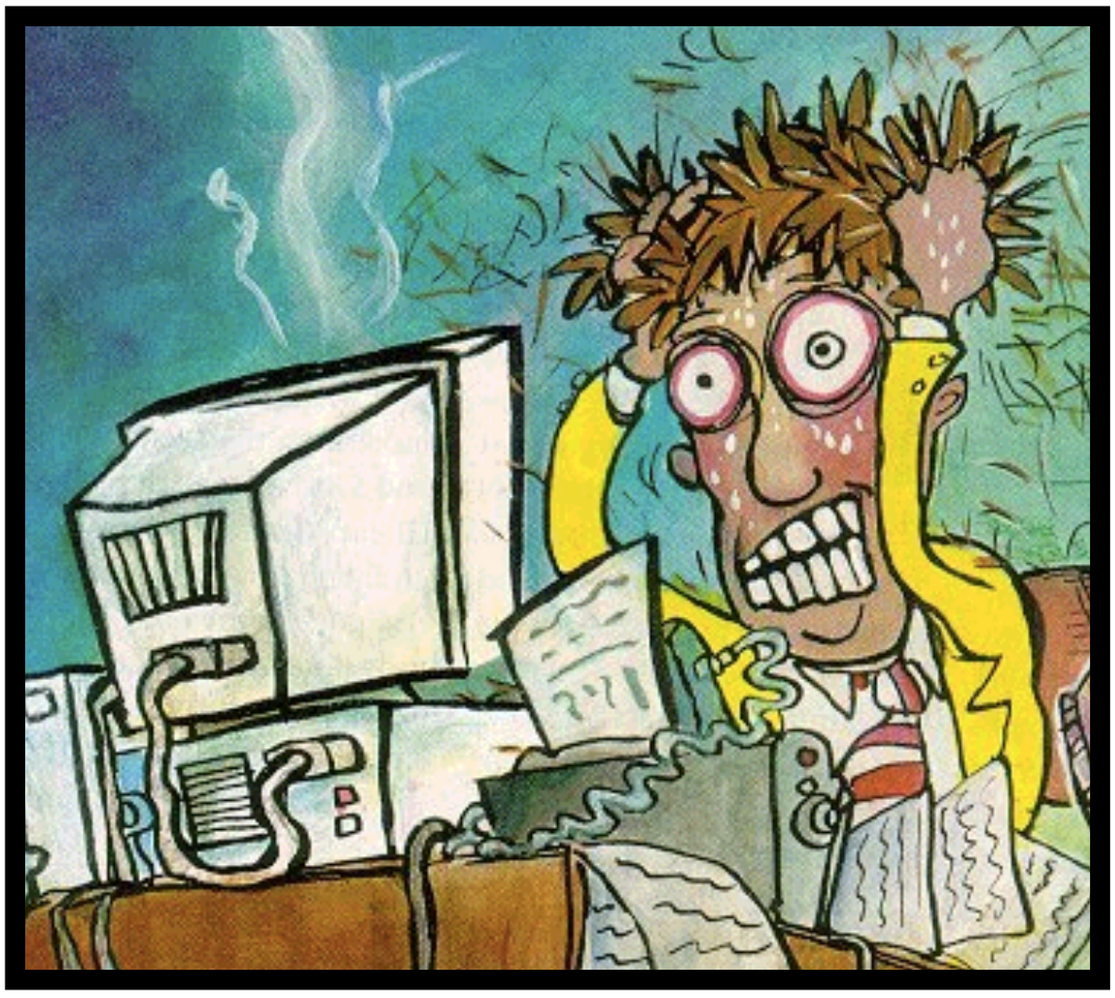
message reorder

machine crash

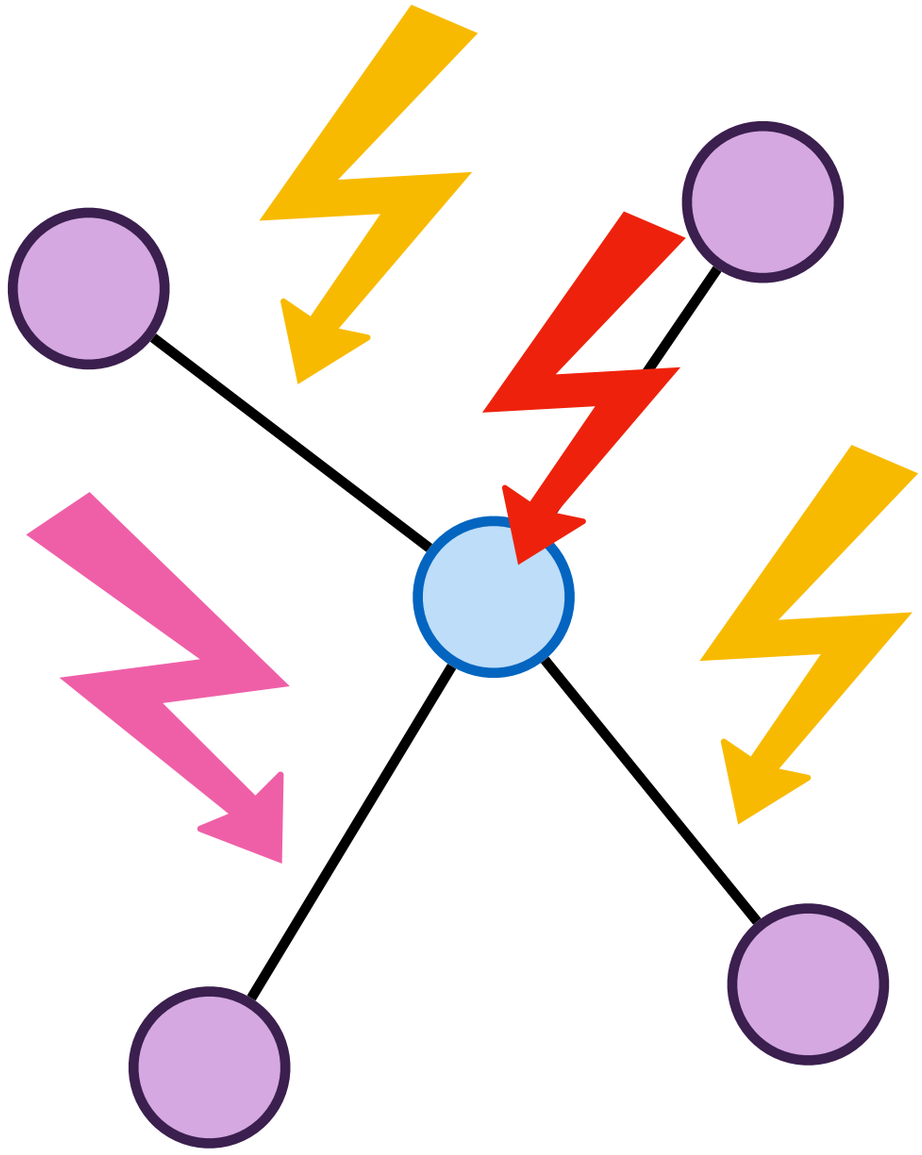
machine reboot

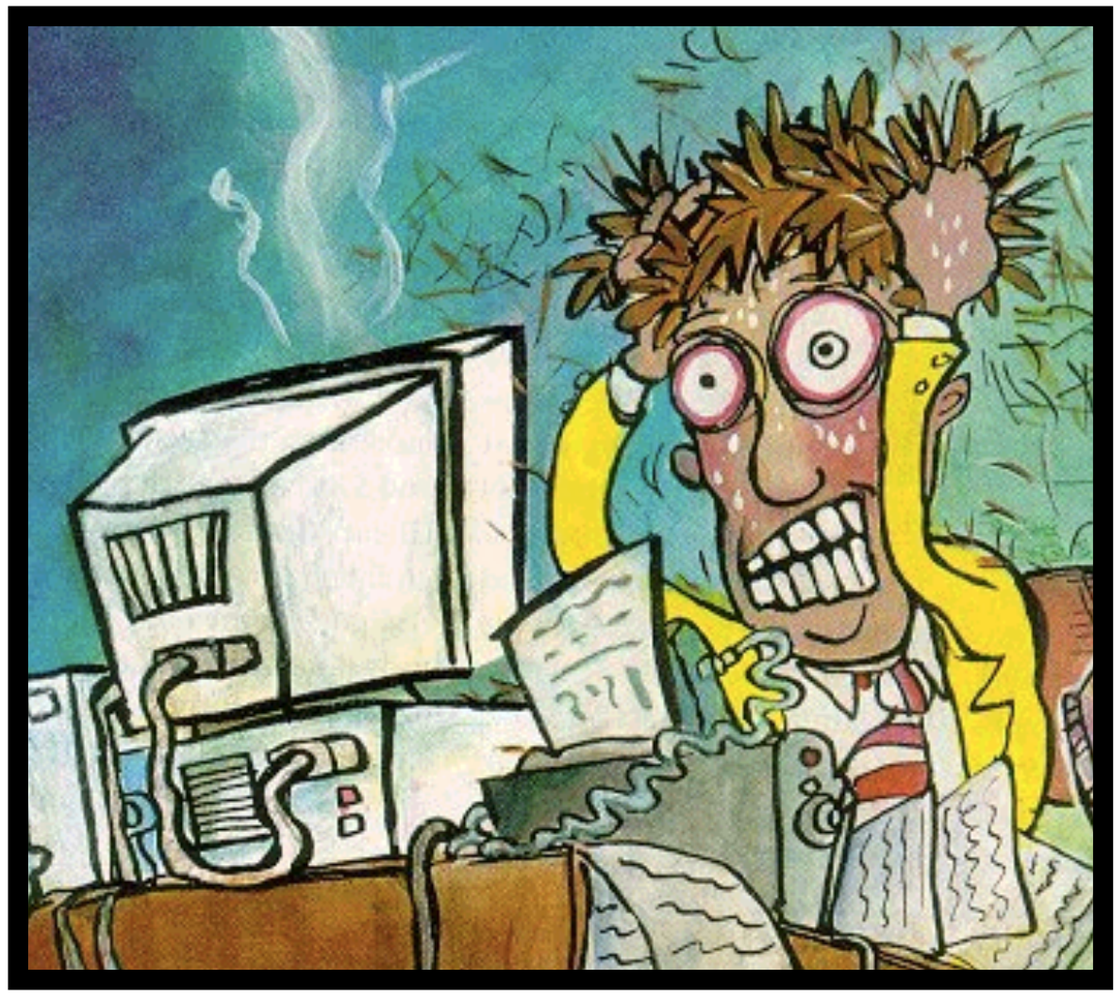
How distributed systems fail





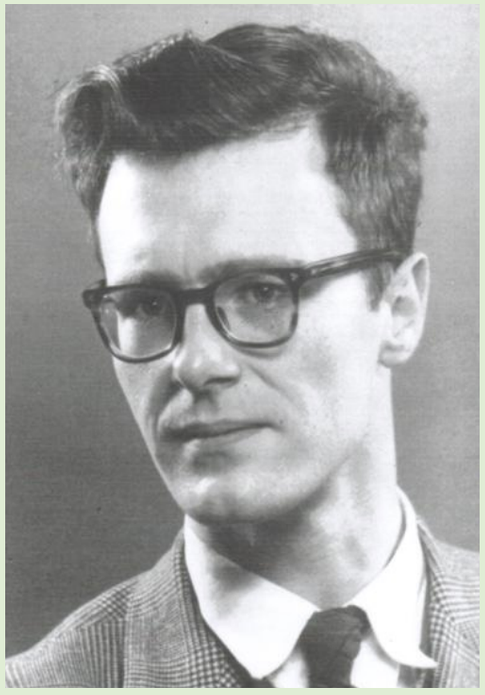
How distributed systems fail





Too many possible behaviors to effectively test!

How distributed systems fail



When exhaustive testing is impossible, our trust can only be based on proof.

Edsger W. Dijkstra
Under the Spell of Leibniz's Dream

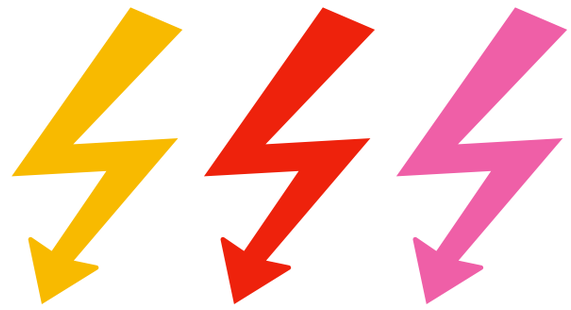
Too many possible behaviors to effectively test!

Toward verified distributed systems

Toward verified distributed systems

Formalize *network semantics*

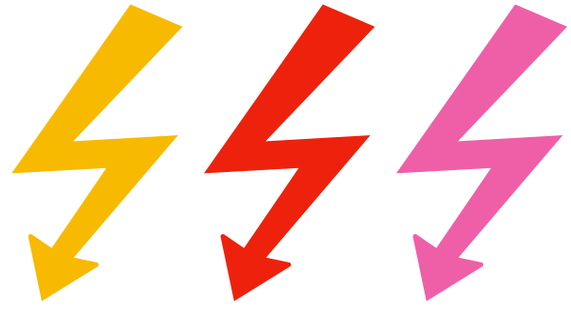
capture how faults can occur



Toward verified distributed systems

Formalize *network semantics*

capture how faults can occur

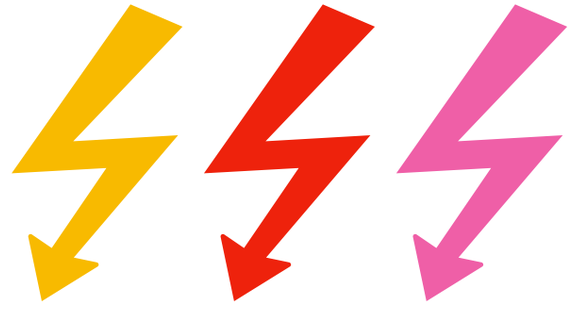


Separate app / fault reasoning

Toward verified distributed systems

Formalize *network semantics*

capture how faults can occur



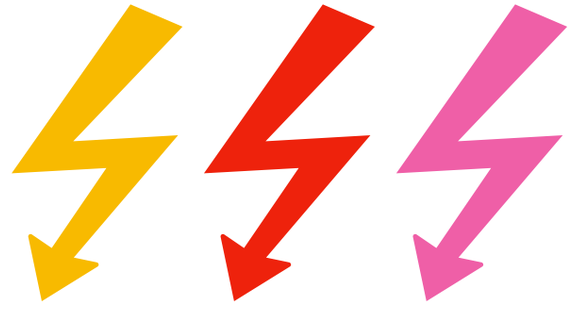
Separate app / fault reasoning

develop and prove in simple fault model

Toward verified distributed systems

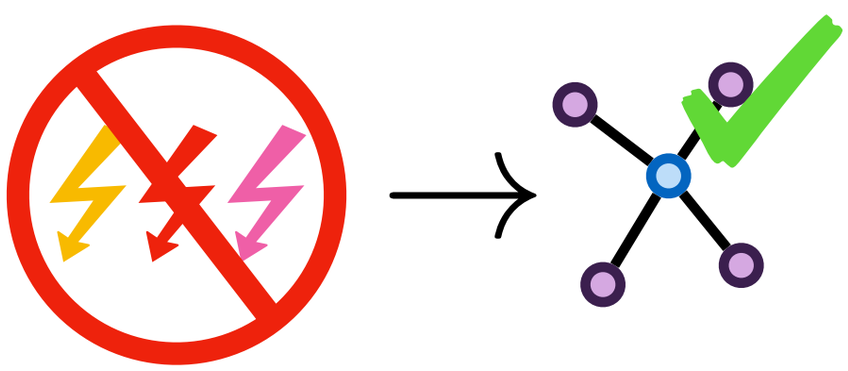
Formalize *network semantics*

capture how faults can occur



Separate app / fault reasoning

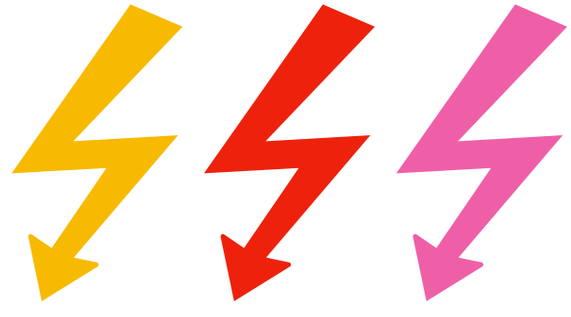
develop and prove in simple fault model



Toward verified distributed systems

Formalize *network semantics*

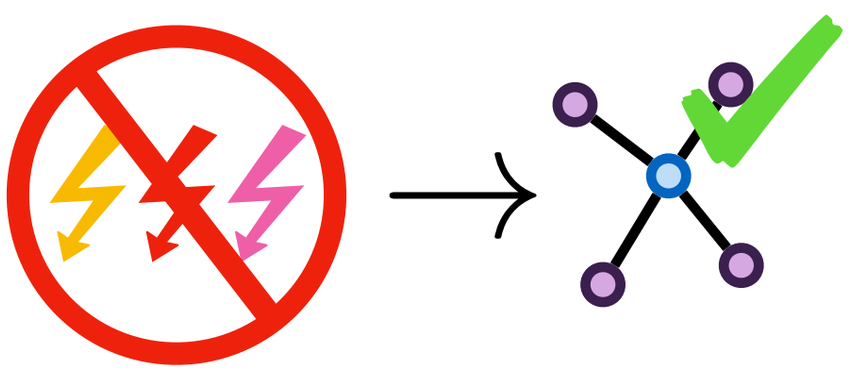
capture how faults can occur



Separate app / fault reasoning

develop and prove in simple fault model

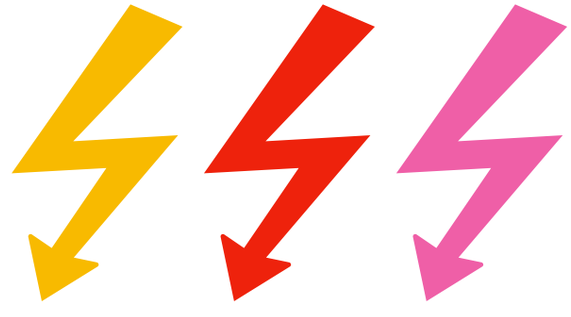
apply generic verified fault handling



Toward verified distributed systems

Formalize *network semantics*

capture how faults can occur

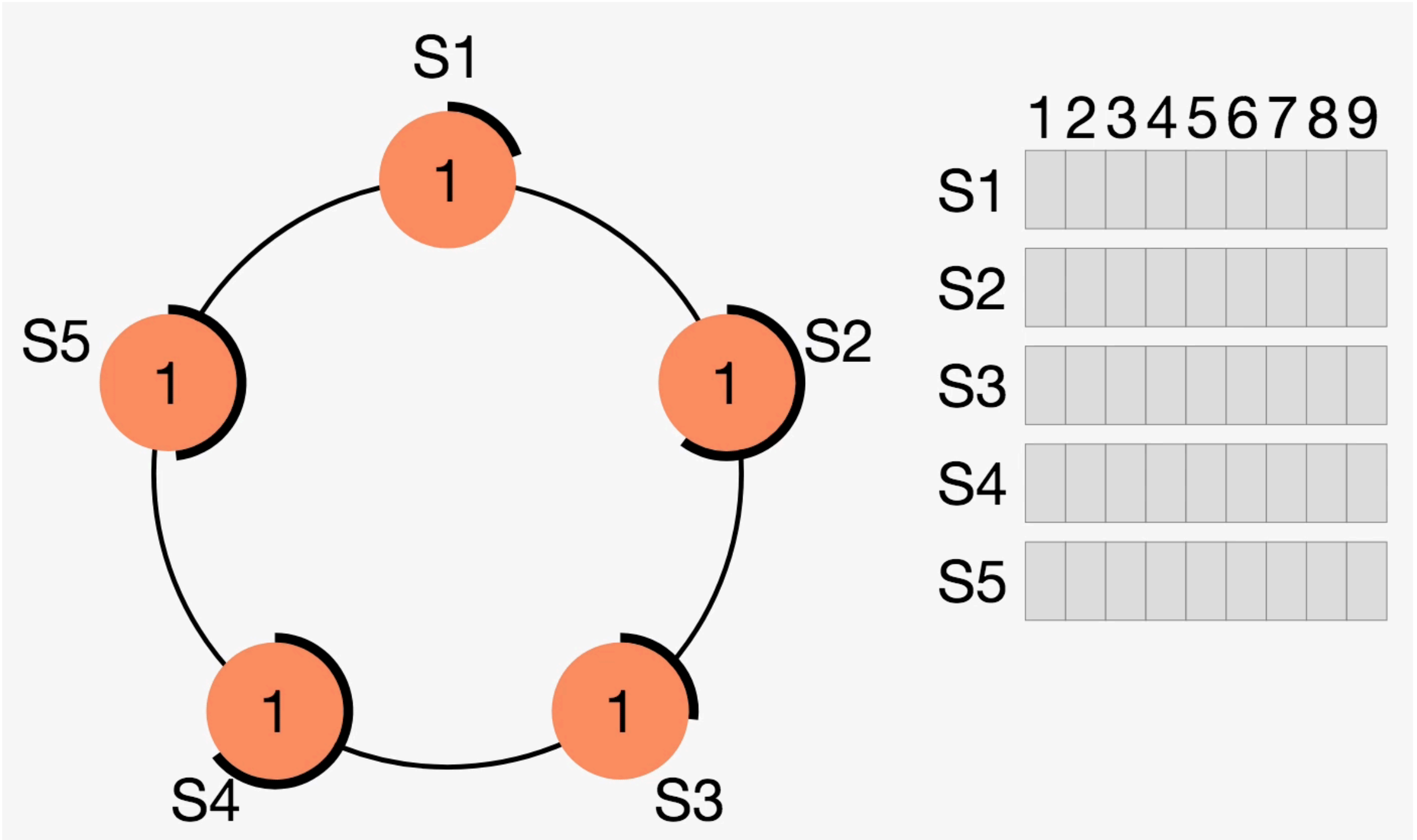


Separate app / fault reasoning

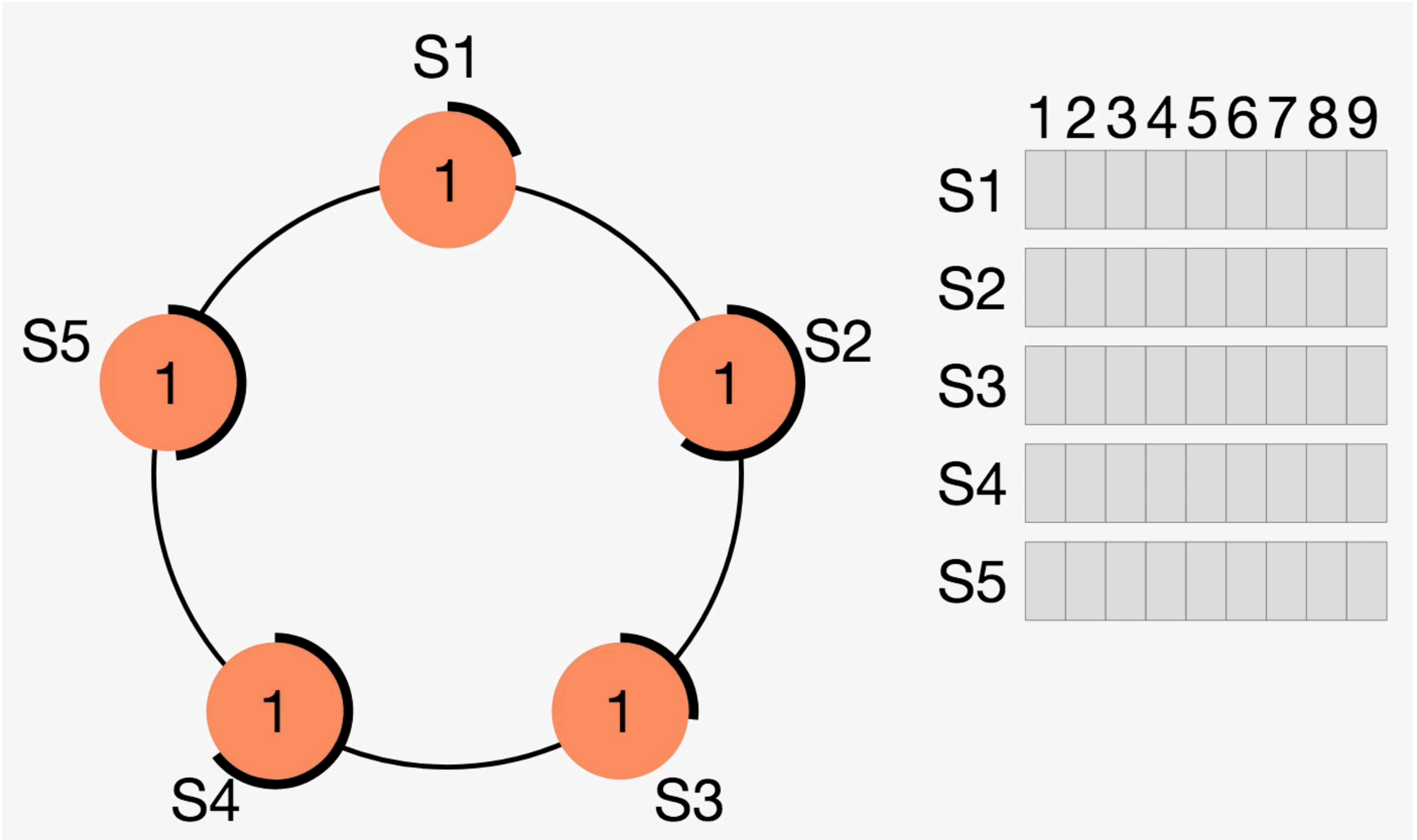
develop and prove in simple fault model

apply generic verified fault handling

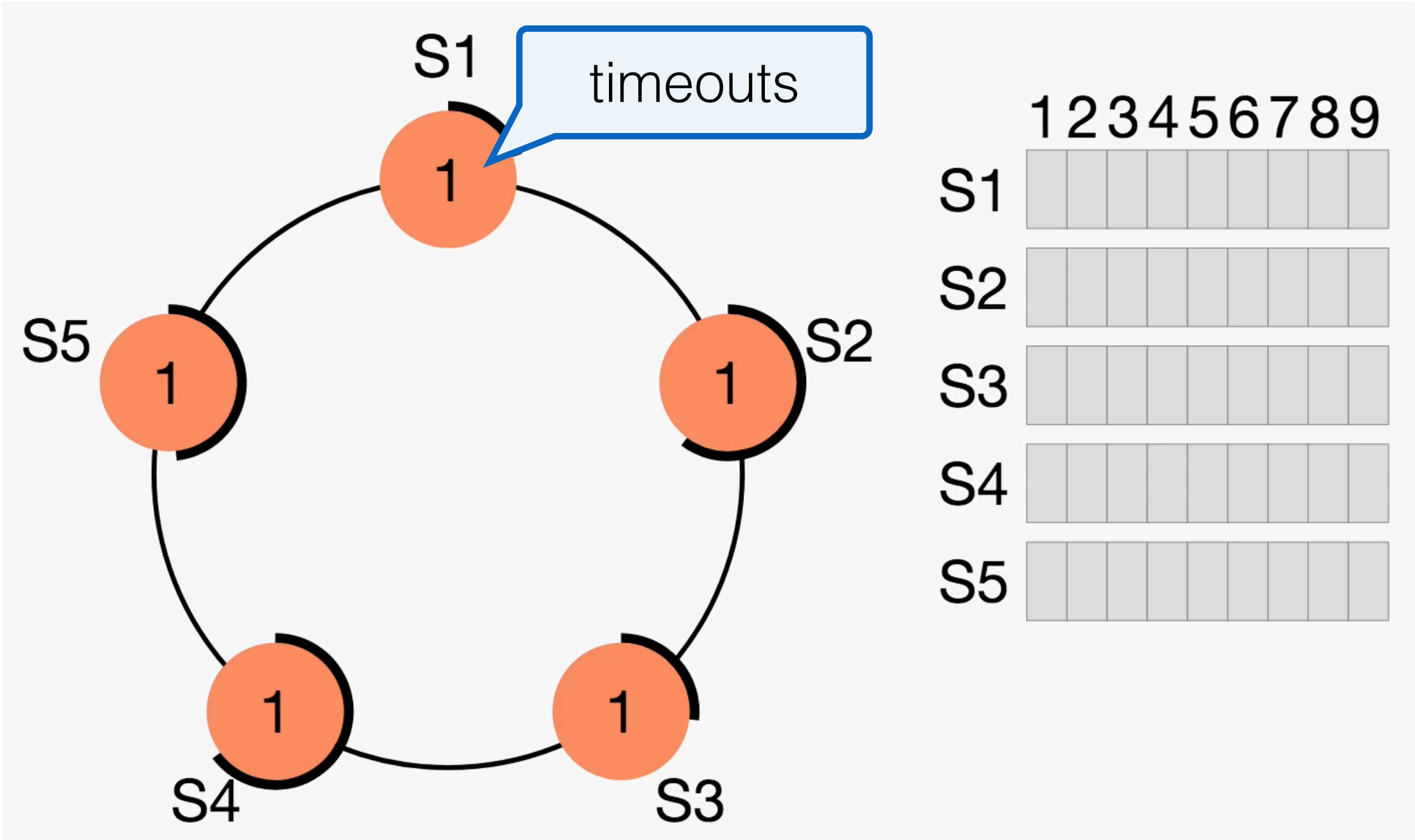
Formalizing distributed systems



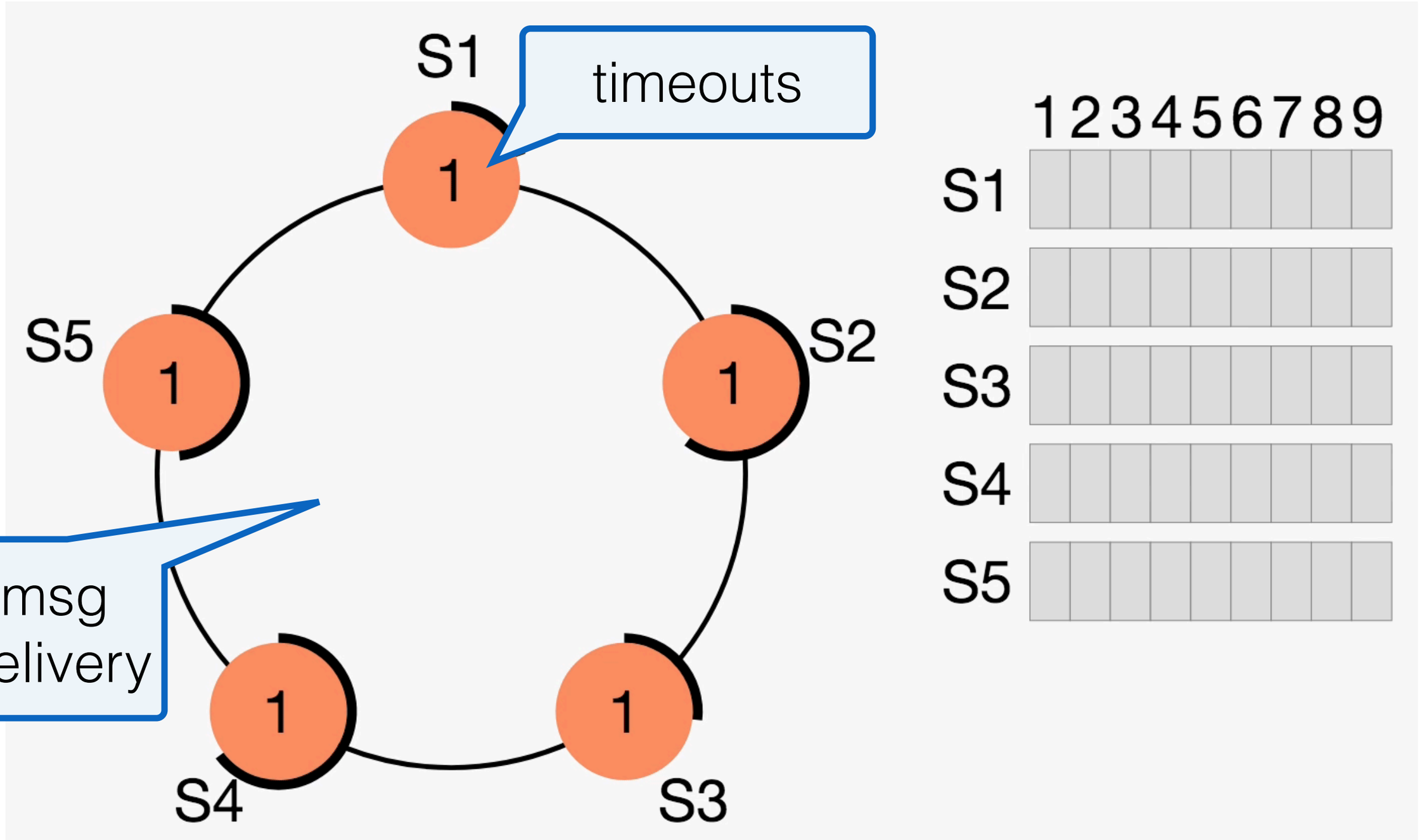
Formalizing distributed systems



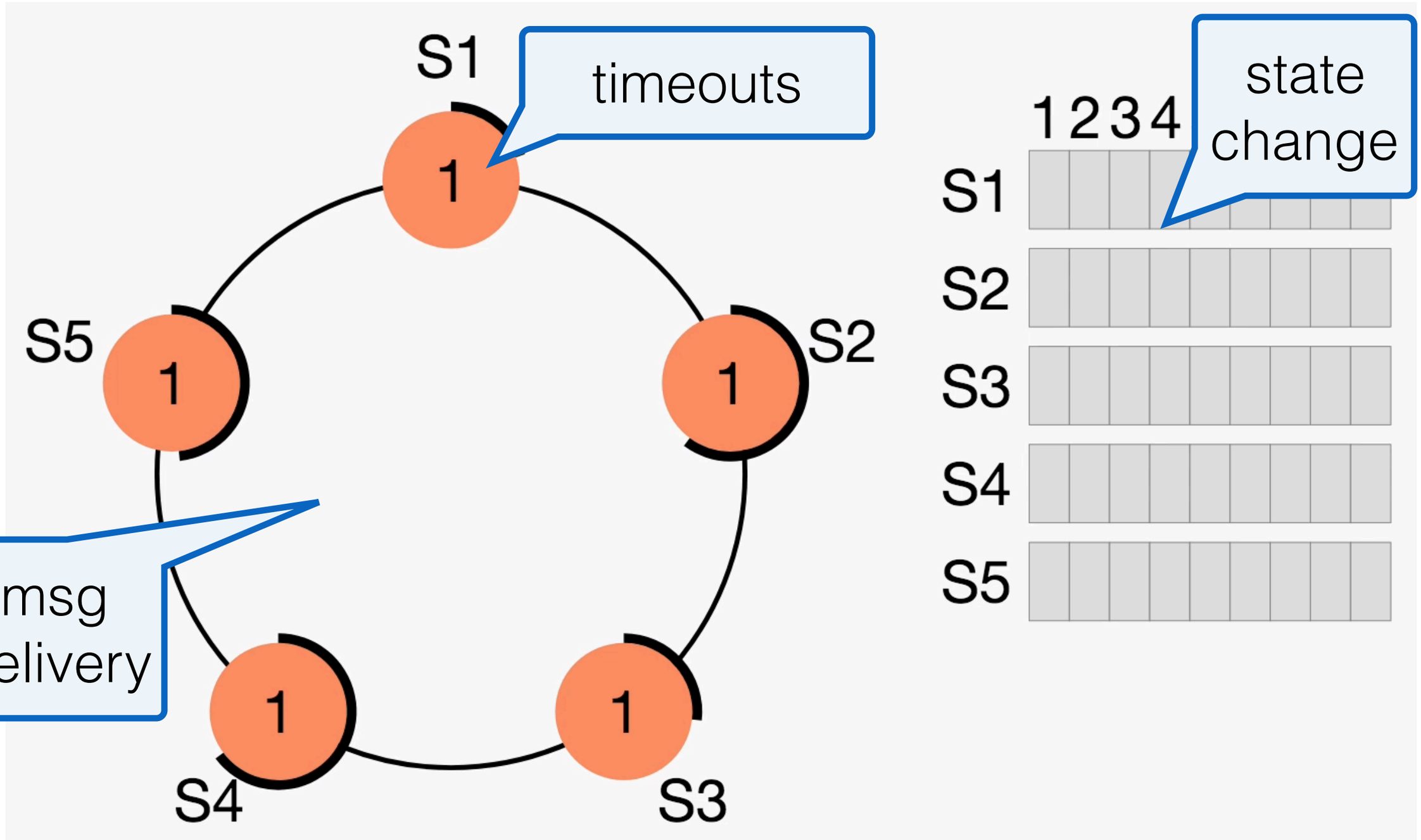
Formalizing distributed systems



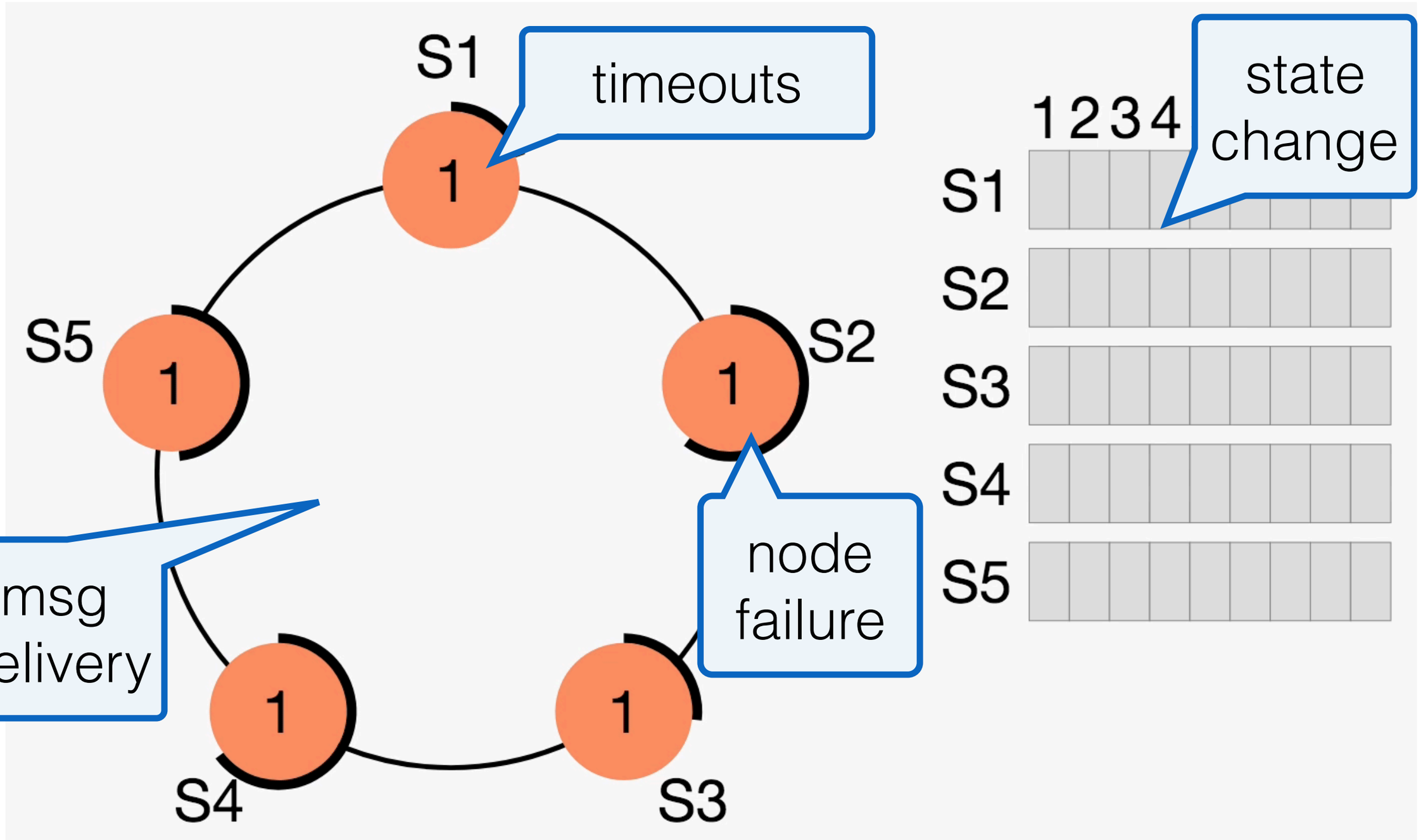
Formalizing distributed systems



Formalizing distributed systems



Formalizing distributed systems



Formalizing distributed systems