Next Economic Crisis? It’s the Network!

Roger Wattenhofer


KAMBROOK


McKay Brothers


KAMBROOK


TENSION
emano

Part 1
Financial Networks

Joint work with Pal Andras Papp and Beni Egressy


IT'S THE
ECONOMY
STUPID!

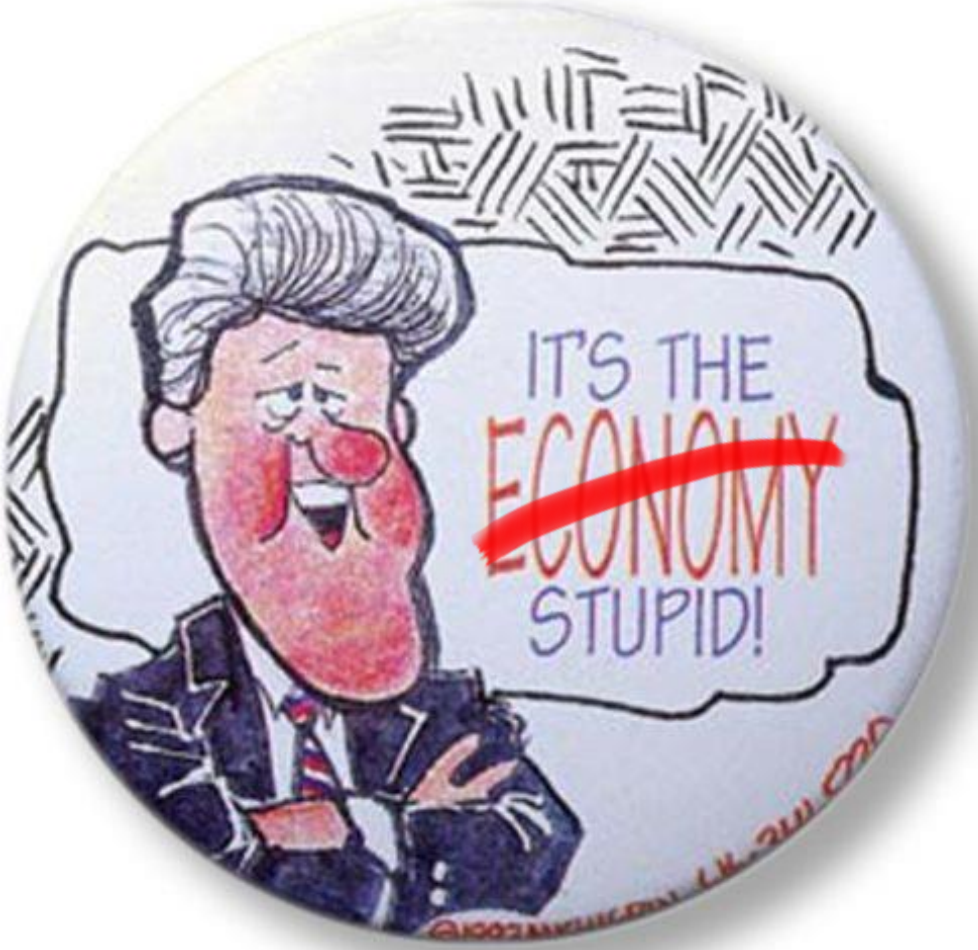
economic crisis

=

many companies involved

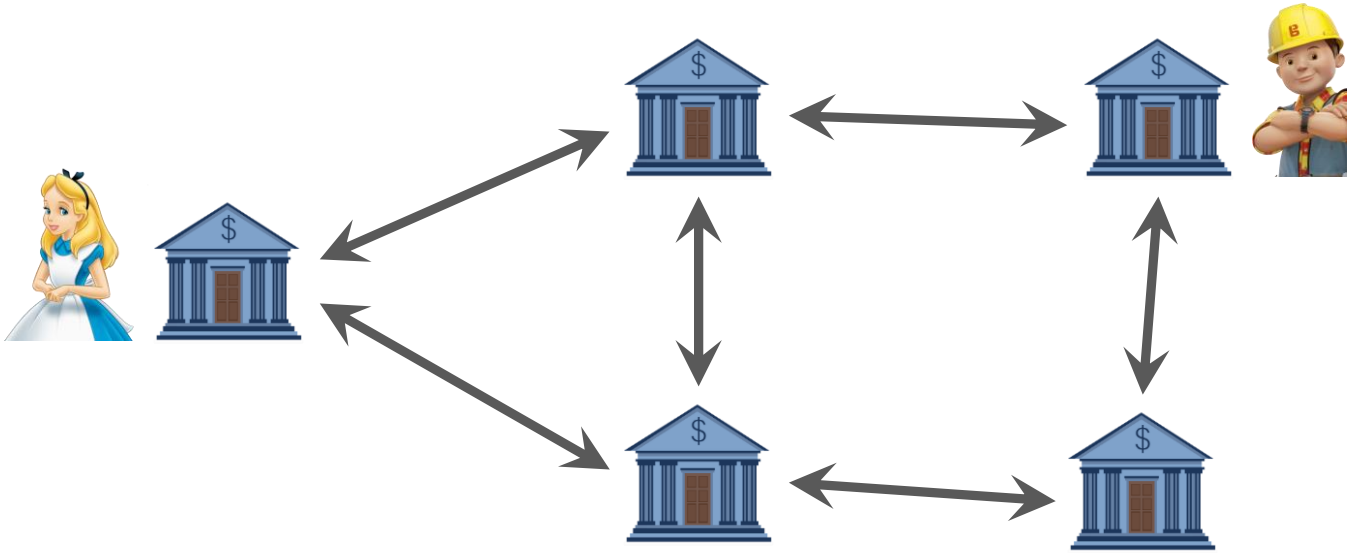
=

network

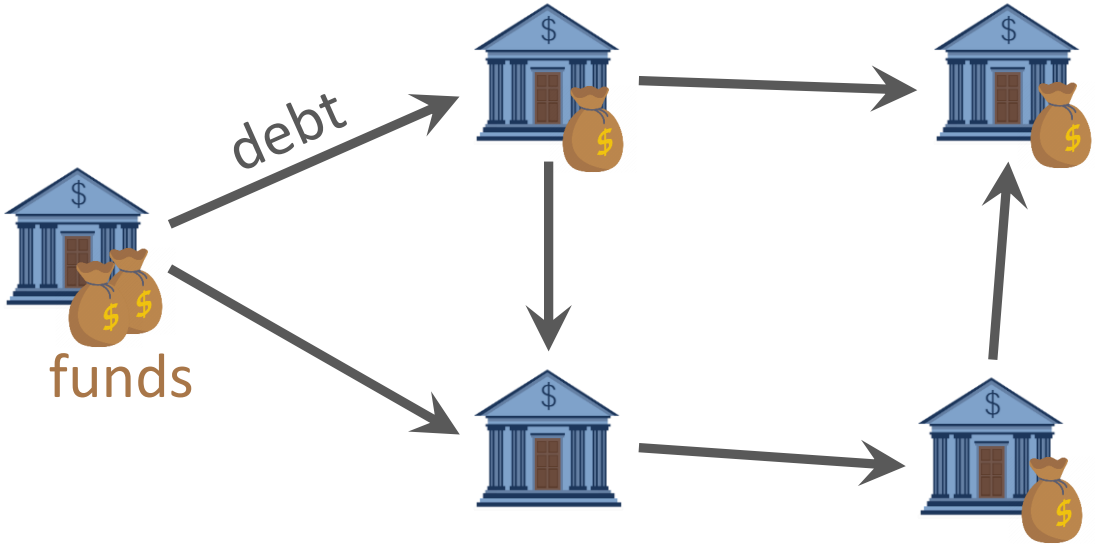


NETWORK

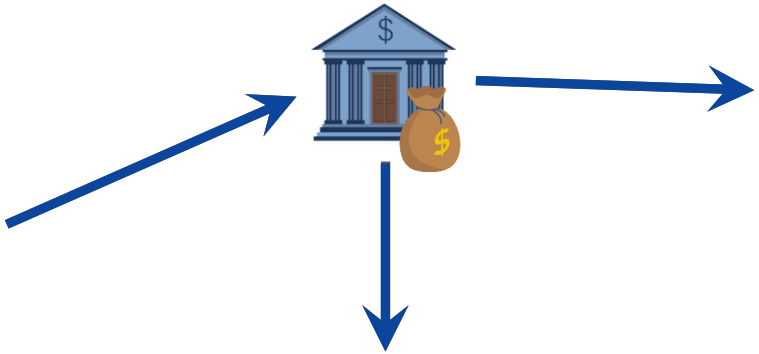
Financial Network



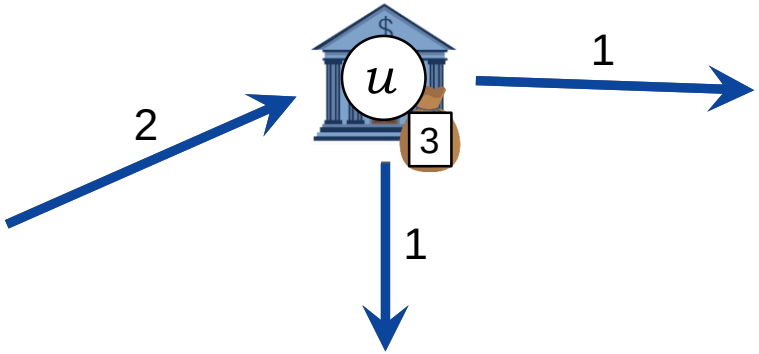
Financial Network



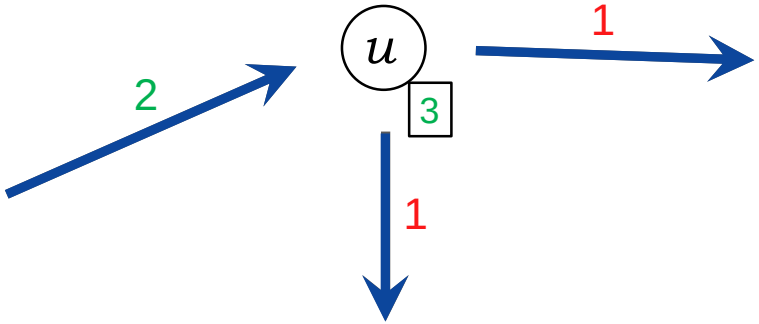
Assets, Liabilities, Default, and Recovery Rate



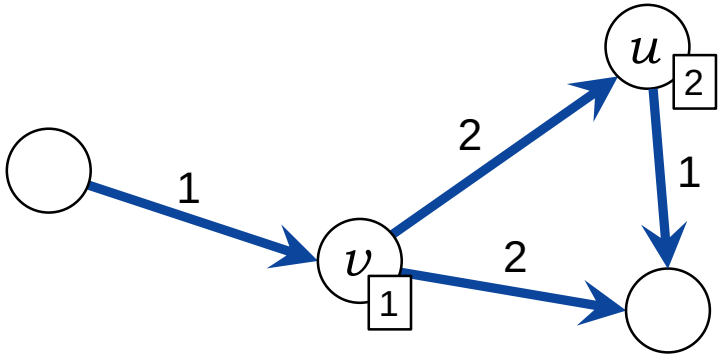
Assets, Liabilities, Default, and Recovery Rate



Assets, Liabilities, Default, and Recovery Rate



Assets, Liabilities, Default, and Recovery Rate



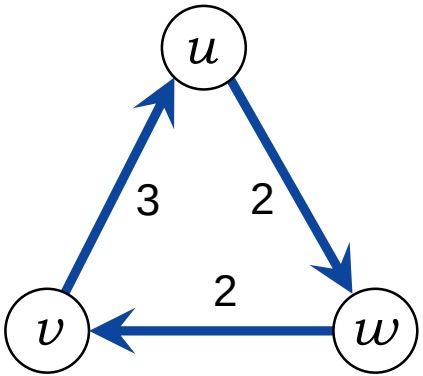
$$a_u \geq l_u \Rightarrow r_u = 1$$

$$a_v < l_v \Rightarrow r_v = \frac{a_v}{l_v} = \frac{2}{4} = \frac{1}{2}$$

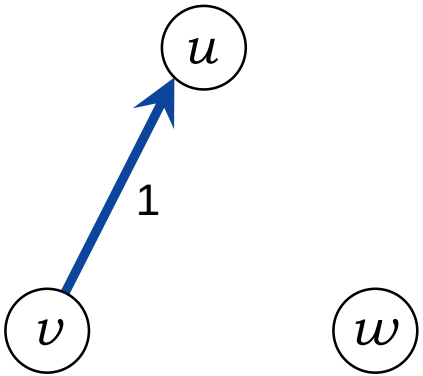
Debt Cycles


FAMILY ROOM
(ADDITION)
45'-8"
SHOWER
BATHROOM
WALK-IN CLOSET
HALL
BEDROOM
KITCHEN
EXIST. JOISTS
EXIST. GUARD

Reducing Debt Cycles



Reducing Debt Cycles



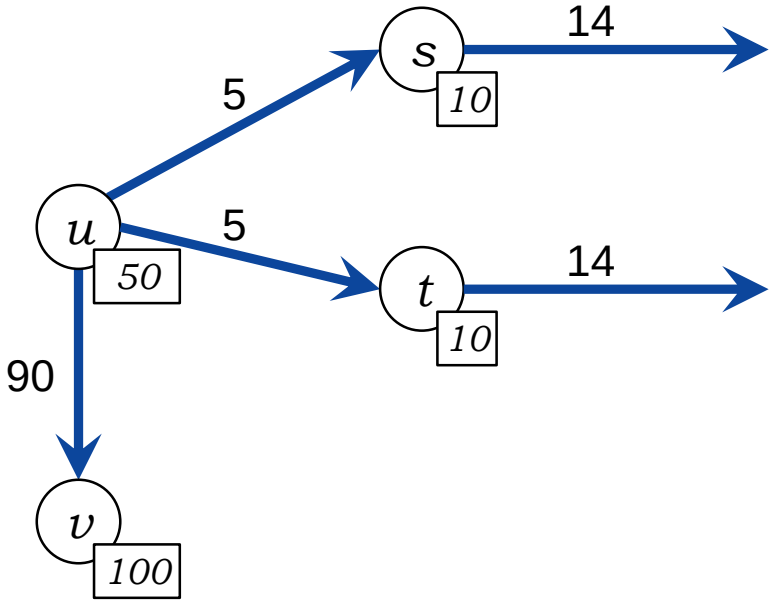
Service companies are doing this.

Without Privacy!

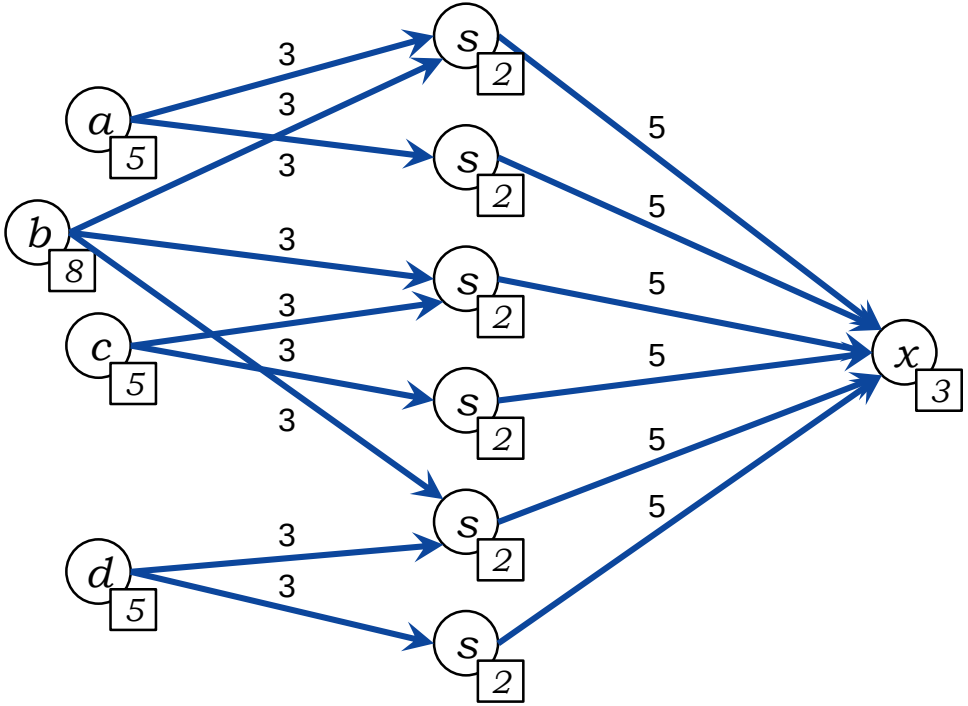
Bailouts


FAMILY ROOM
(ADDITION)
SHOWER
BATHROOM
WALK-IN CLOSET
HALL
BEDROOM
KITCHEN
EXIST. JOISTS

Too Big to Fail?



Bailouts on a Budget (of 3)



Bailouts are NP hard.

Conditional Debt

Debt = “Long” Position (Positive)

Conditional Debt = “Short” (Negative)

Short Positions

ABS: Asset-Backed Securities

CDO: Collateralized Dept Obligations

CDS: Credit Default Swaps

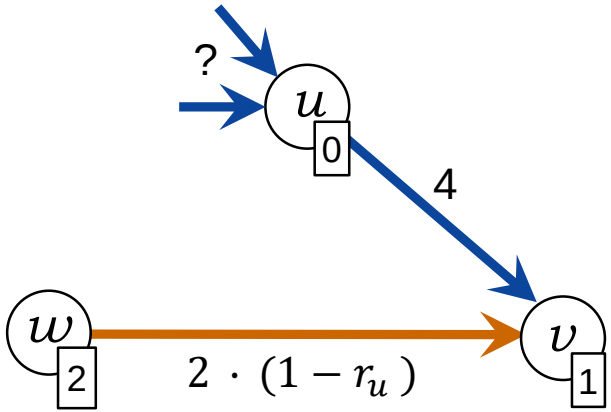
CLS: Collateralized Loan Obligations

MBS: Mortgage-Backed Securities

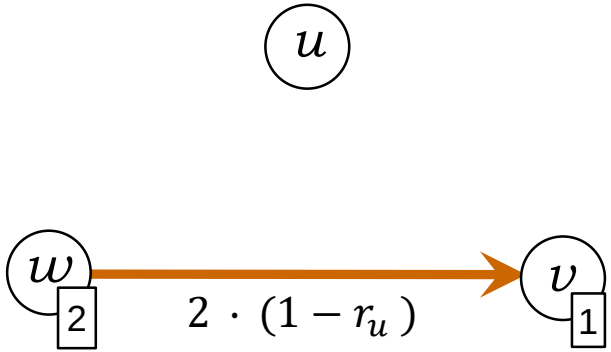
…

“Financial Weapons of Mass Destruction” (Warren Buffet)

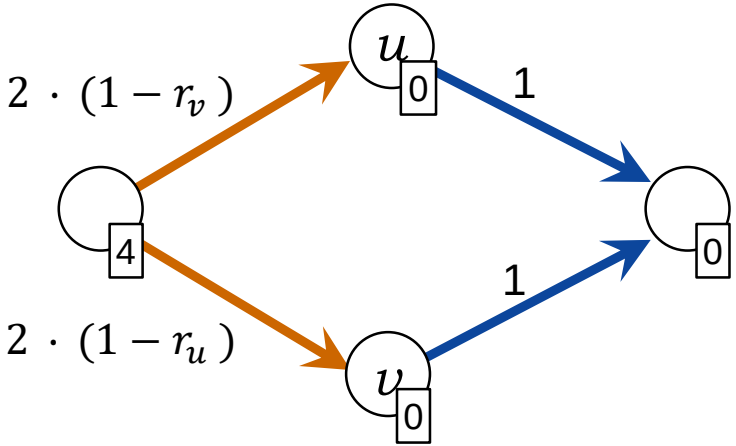
Conditional Debt Contracts



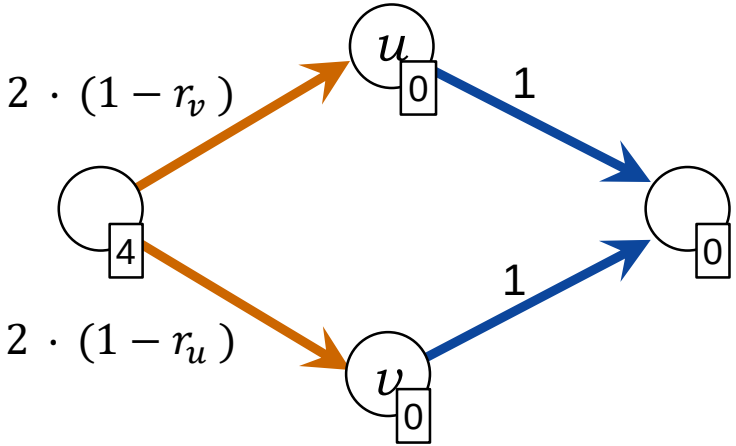
Conditional Debt Contracts



Example



Example

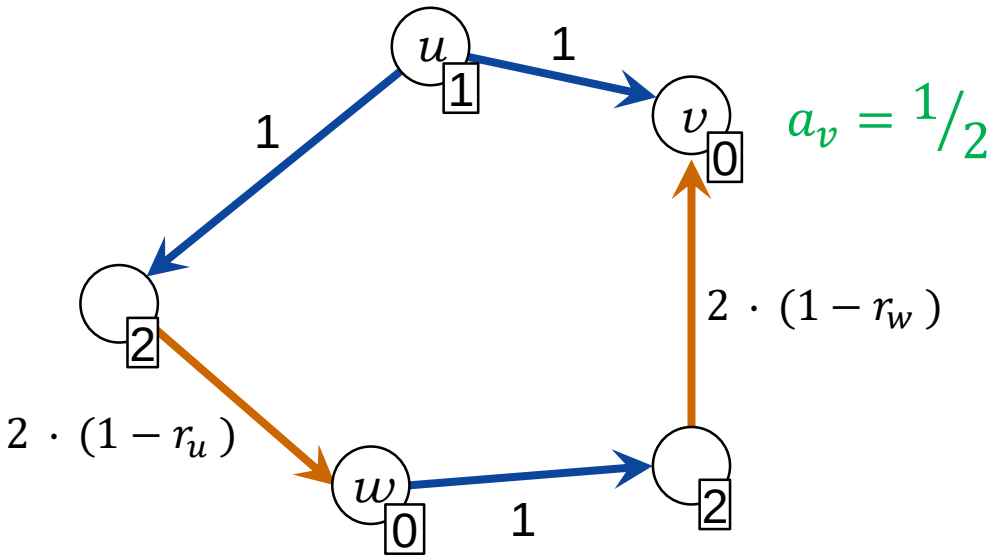


r_u	r_v
1	0
0	1
$2/3$	$2/3$

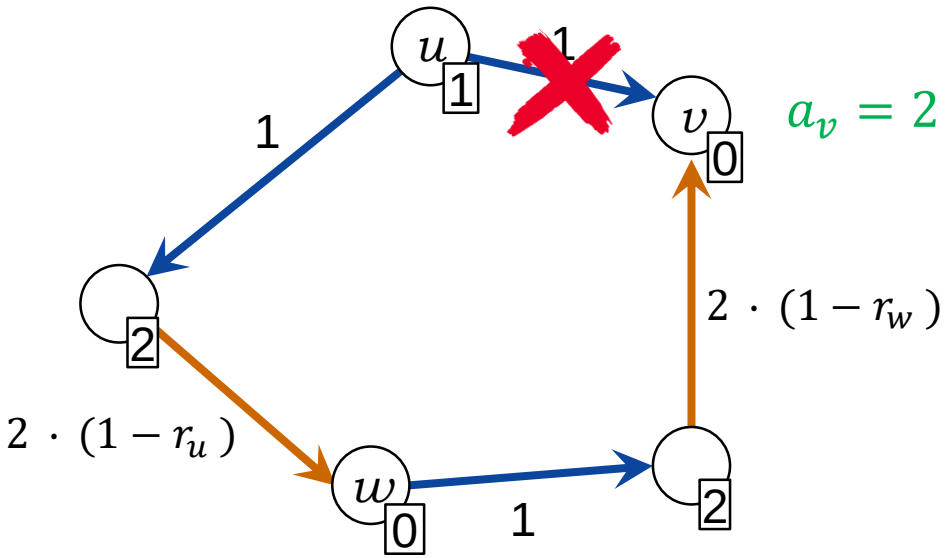
Timing Matters.

Improve Situation

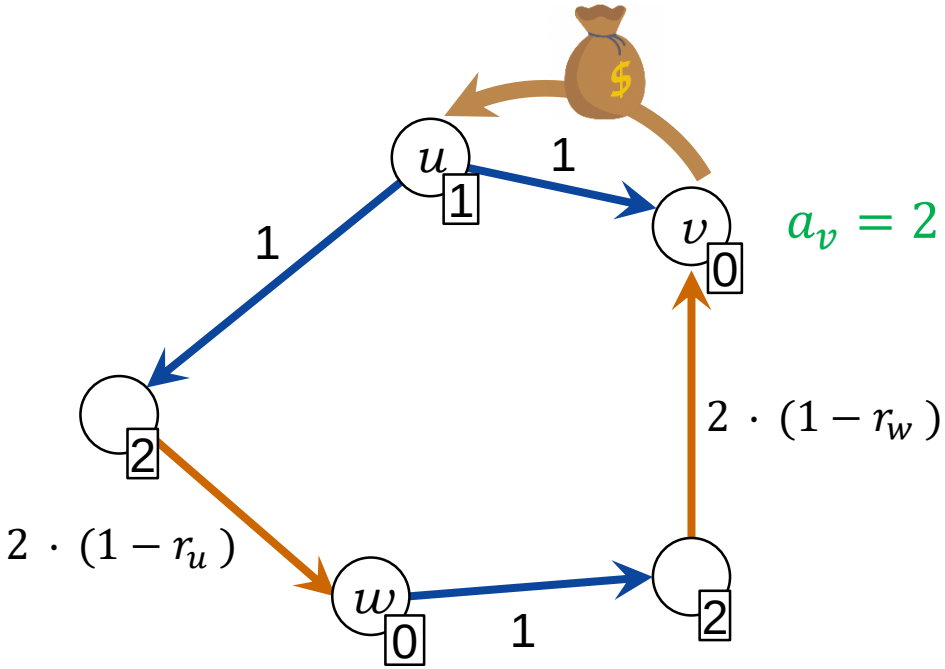
Can Bank v Improve?



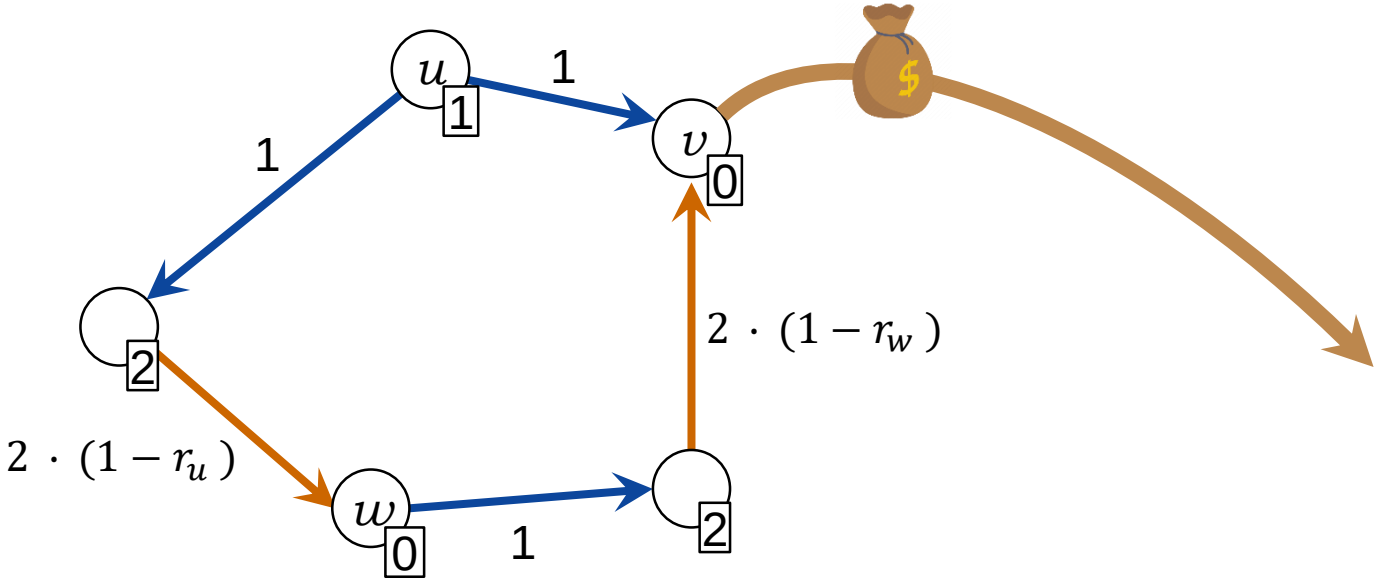
Can Bank v Improve?



Can Bank v Improve?



Can Bank v Improve?



A Loss Can Be a Win.

The Atlantic

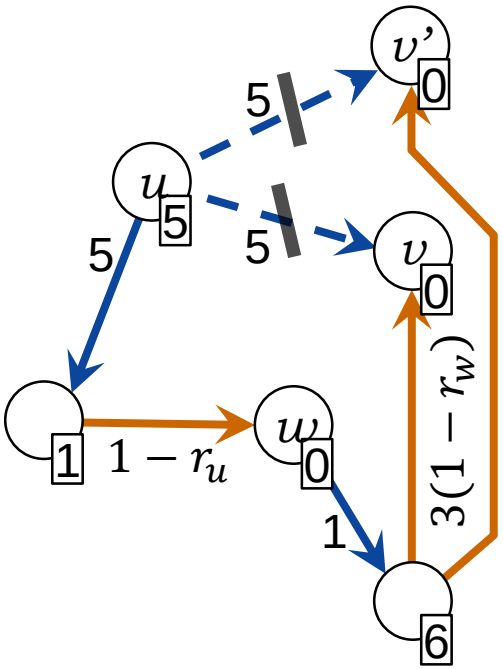
BUSINESS

How to Make Money for Nothing Like Wall Street

Credit default swaps might not be financial WMDs anymore, but Wall Street can still game them to make guaranteed profits.

MATTHEW O'BRIEN OCTOBER 24, 2013

Prisoner's Dilemma



v' \ v		
	3	4
	1.5	2.66

Optimization

Optimize What?

Preferred by highest number of banks

Smallest amount of total debt unpaid

Smallest percentage of liabilities in the system unpaid

Best for a specific bank

Most representative of the solution space

Most balanced for two alliances of banks

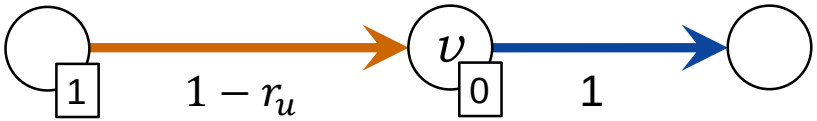
Smallest number of defaults

Worst for a specific bank

All these (and more) are NP hard.

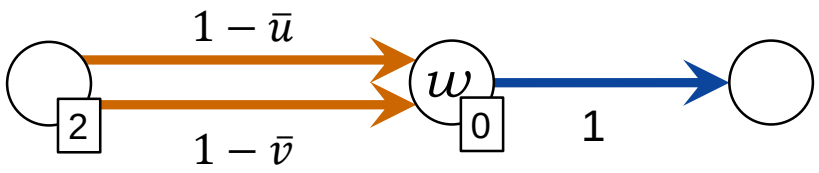
Building Circuits: NOT Gate

u $r_u \in \{0,1\}$



$$r_v = NOT\ \ r_u$$

Building Circuits: OR Gate



$$r_w = r_u \ OR \ r_v$$

Financial Networks are Turing-Complete.

Part 2
The Future

Joint work with Jakub Sliwinsky and Zeta Avarikioti

Banker: “Blockchain: The Biggest Thing.”

Roger: “Even Bigger than the Internet?”

Banker: “Much Bigger.”


Digital
Transformation

Financial Transaction Confirmation takes about 1 Day

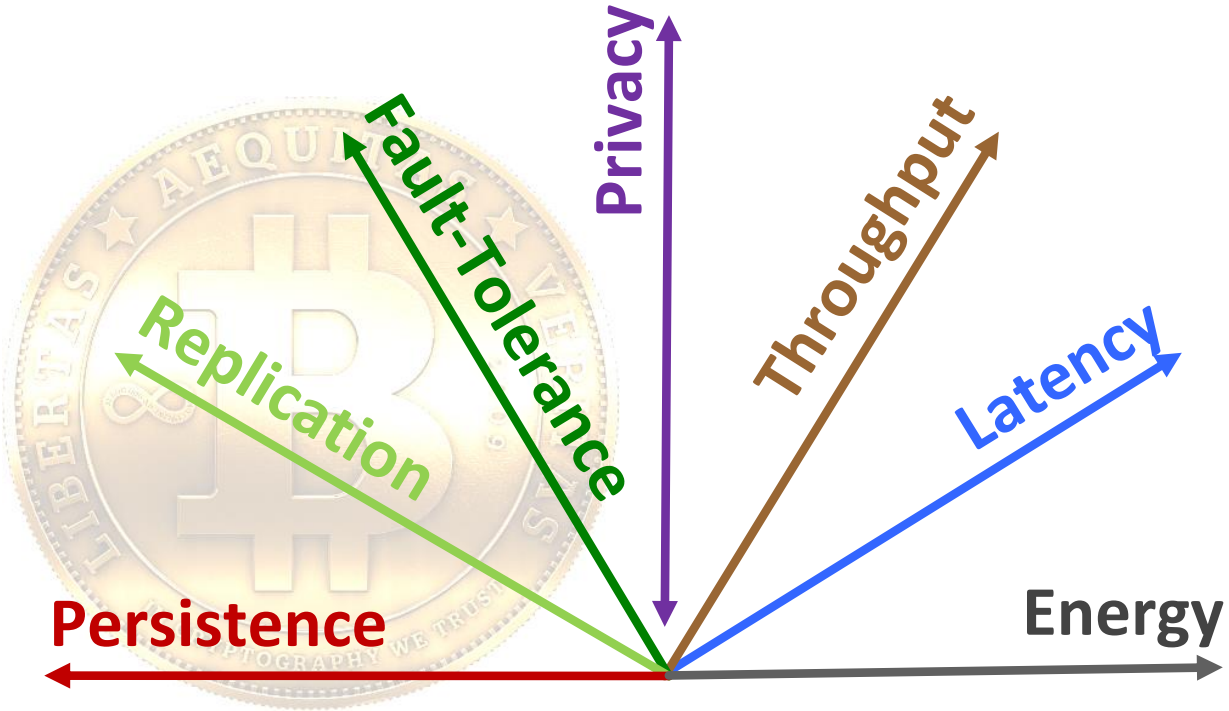
Trust: Which Computer(s) Store Your Account Balance?


LIBERTAS
AEQUITAS
VERITAS
2009

Central Bank Digital Currency (CBDC)


STATUS DOLLAR ECOIN CRYPTOGRAPHIC
USD₵
EST 2014

Some Blockchain Dimensions



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

"The problem of course is the payee can't verify that one of the owners did not double-spend the coin."

"We need a system for participants to agree on a single history of the order in which [transactions] were received."

no double-spending

$\neq$

single order

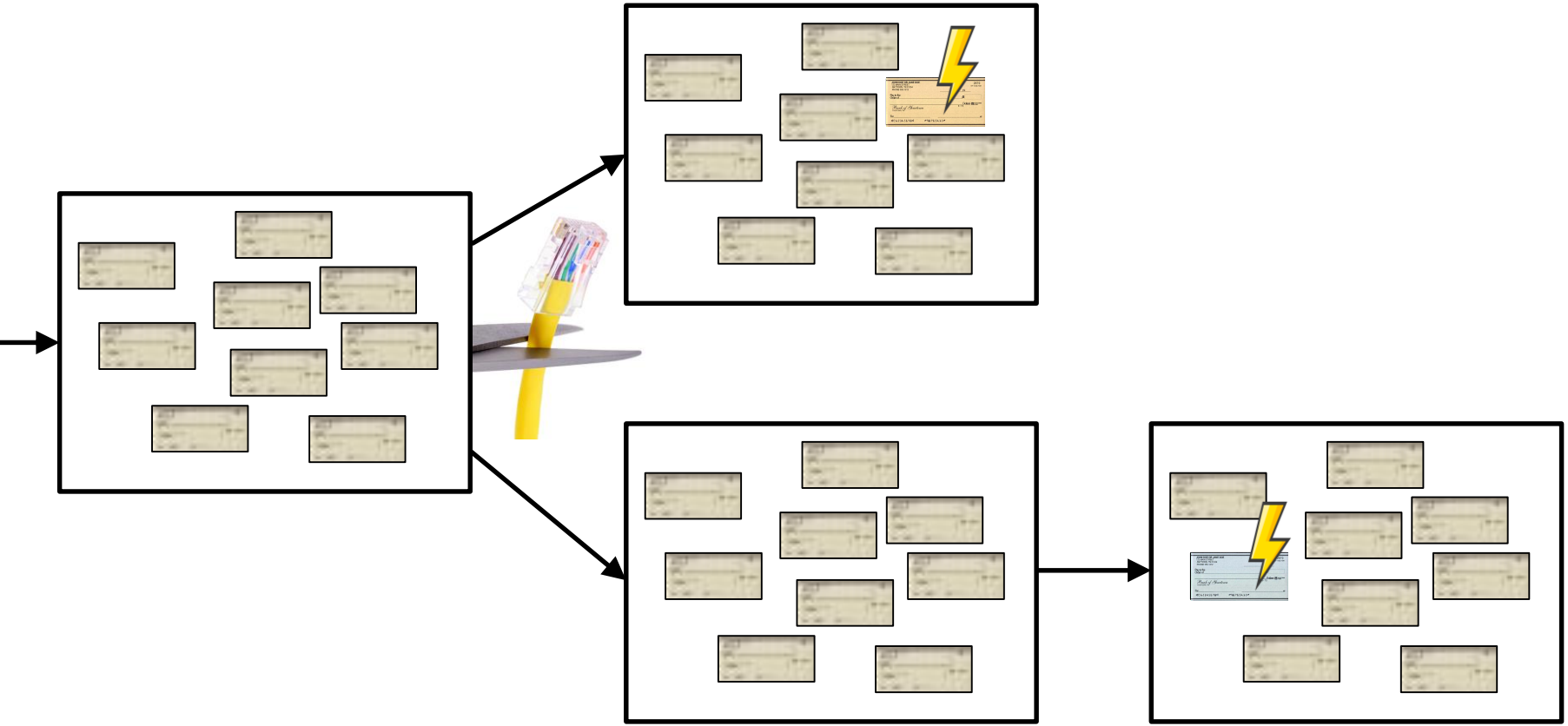
$=$

consensus

Double-Spending

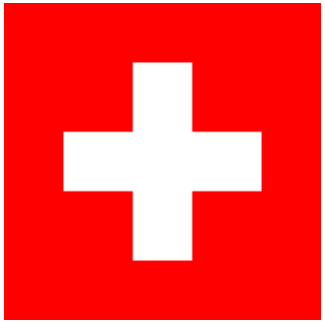
Blockchains Solve Double-Spending Problem

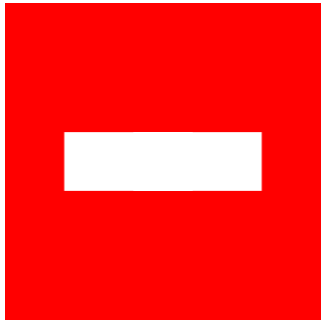
What About Network Outages?



Asynchrony


FAMILY ROOM
(ADDITION)
45'-8"
SHOWER
BATHROOM
WALK-IN CLOSET
KITCHEN
HALL
BEDROOM
EXIST. JOISTS
EXIST. GUARD
PROVIDE VENTILATION





Unchangeable
Market Cap

Anonymous?
Permissionless?
Scalable = Secure?

Asynchrony
Finality
Throughput
Energy (PoW)
Smart Contracts
Unchangeable

Many Alternatives

	PBFT[1]	HoneyBadger BFT[10]	Broadcast-based[5]	Bitcoin and Ethereum[14]	Ouroboros[7]	Algorand[2]	ABC
Permissionless				✓	✓	✓	✓
Proof-of-work free	✓	✓	✓		✓	✓	✓
Finality	✓	✓	✓			✓	✓
Asynchronous		✓	✓				✓
Deterministic	✓		✓				✓
Parallelizable			✓				✓
General smart contracts	✓	✓		✓	✓	✓	

Without Consensus

A Non-Consensus Based Decentralized Financial Transaction Processing Model
with Support for Efficient Auditing

by

Saurabh Gupta

A Thesis Presented in Partial Fulfi
of the Requirements for th
Master of

ABC: Asynchronous Blockchain without Consensus

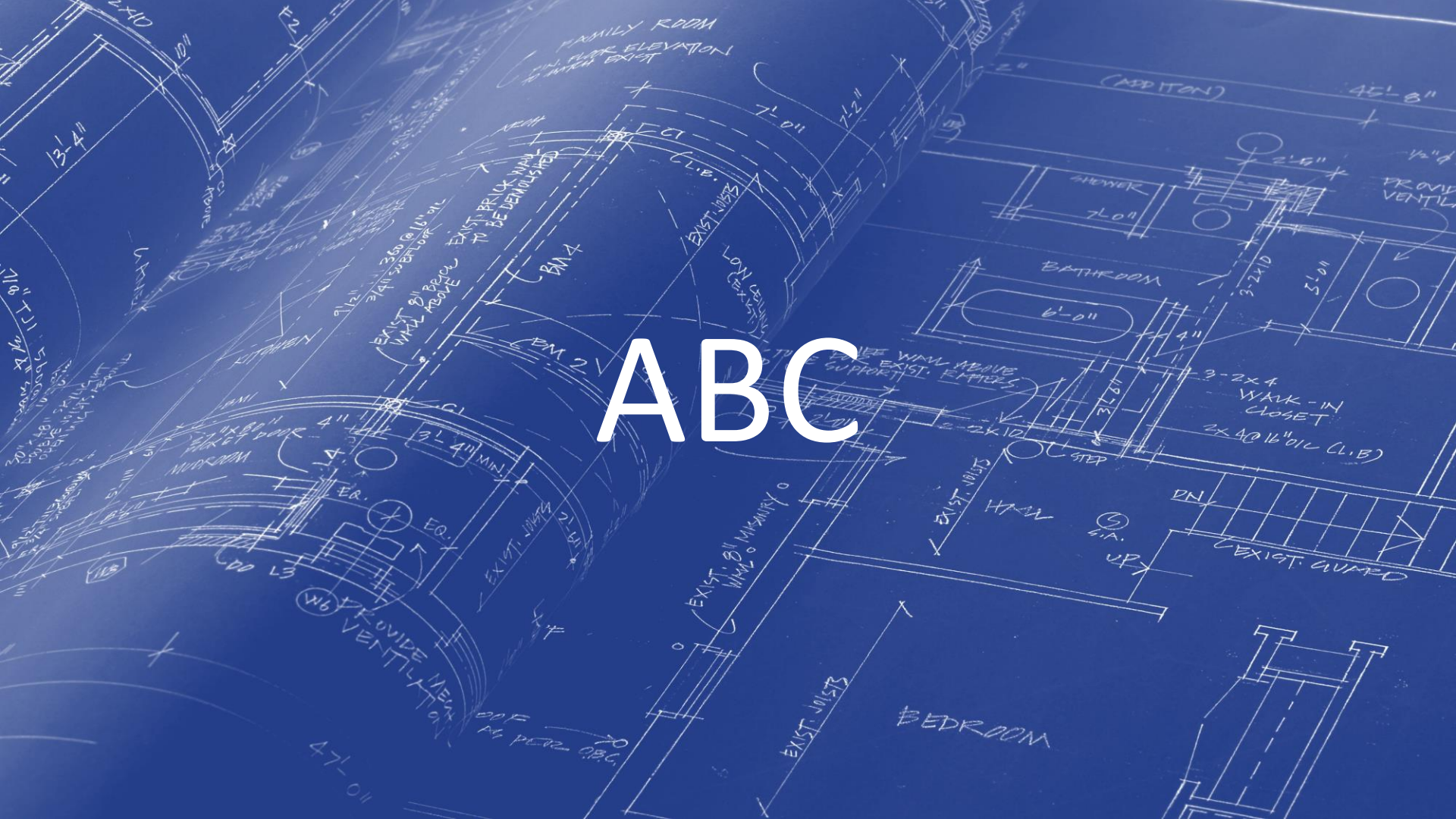
Jakub Sliwinski and Roger Wattenhofer

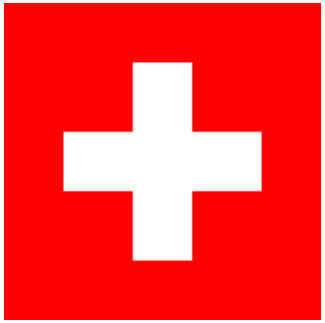
ETH Zurich

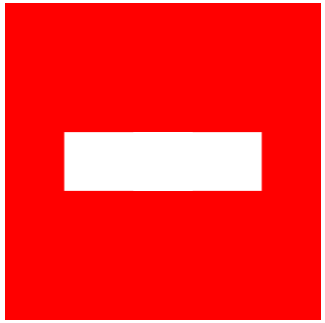
{jsliwinski,wattenhofer}@ethz.ch

onception that a blockchain needs c
ributed property with a remar
consensus is at all ne
called ABC th
ith an a

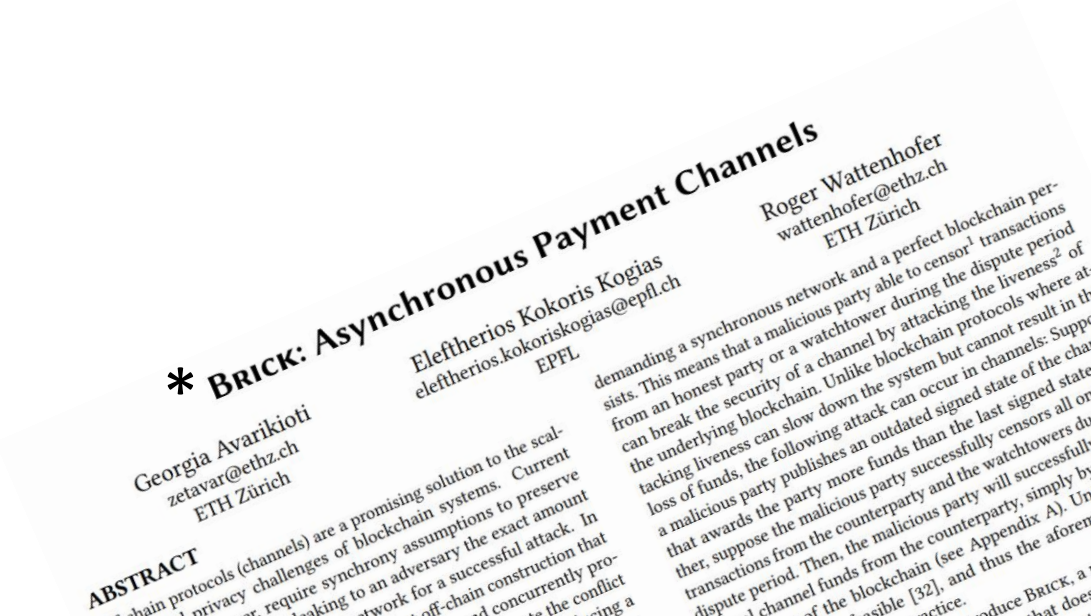
ABC


FAMILY ROOM
(ADDITION)
45'-8"
SHOWER
BATHROOM
WALK-IN CLOSET
KITCHEN
BEDROOM
HALL
EXIST. JOISTS
EXIST. GUARD
PROVIDE VENTILATION
BM 2
BM 4





Asynchronous*
Throughput
Finality
Energy (PoS)
Permissionless
Scalable



* Brick: Asynchronous Payment Channels

Georgia Avarikioti
zetavar@ethz.ch
ETH Zürich

Eleftherios Kokoris Kogias
eleftherios.kokoriskogias@epfl.ch
EPFL

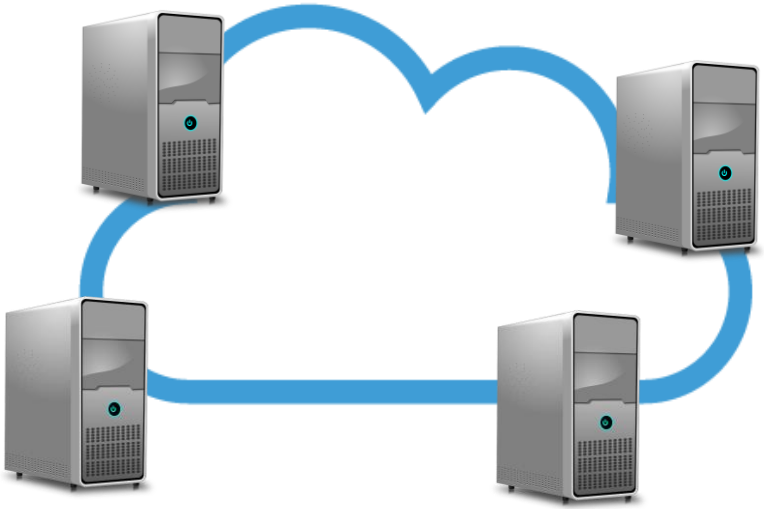
Roger Wattenhofer
wattenhofer@ethz.ch
ETH Zürich

ABSTRACT

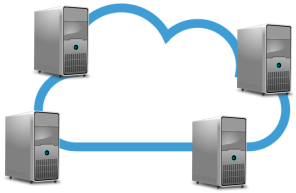
chain protocols (channels) are a promising solution to the scal-
privacy challenges of blockchain systems. Current
r, require synchrony assumptions to preserve
aking to an adversary the exact amount
twork for a successful attack. In
off-chain construction that
d concurrently pro-
g the conflict
ing a

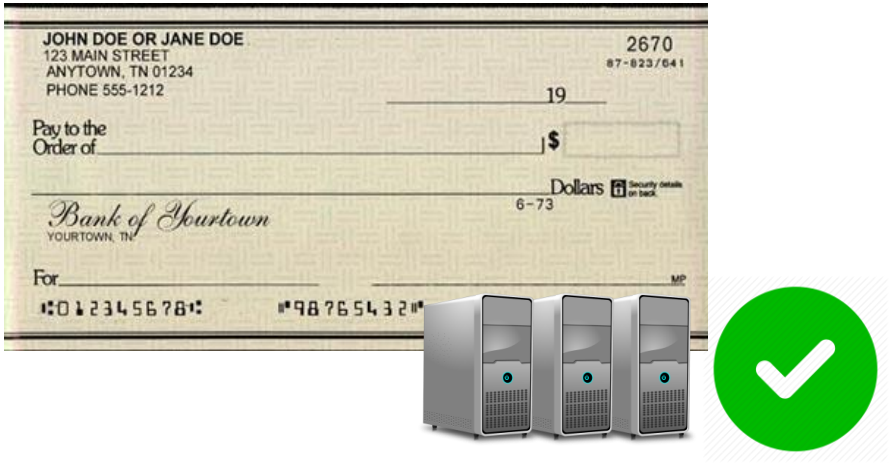
demanding a synchronous network and a perfect blockchain per-
sists. This means that a malicious party able to censor[1] transactions
from an honest party or a watchtower during the dispute period
can break the security of a channel by attacking the liveness[2] of
the underlying blockchain. Unlike blockchain protocols where at-
tacking liveness can slow down the system but cannot result in th
loss of funds, the following attack can occur in channels: Suppo
a malicious party publishes an outdated signed state of the cha
that awards the party more funds than the last signed state
ther, suppose the malicious party successfully censors all o
transactions from the counterparty and the watchtowers du
dispute period. Then, the malicious party will successfully
channel funds from the counterparty, simply by
of the blockchain (see Appendix A). Un
ssible [32], and thus the aforem
ctice.
oduce Brick, a
that does

Permissioned ABC



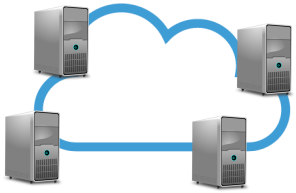
Permissioned ABC

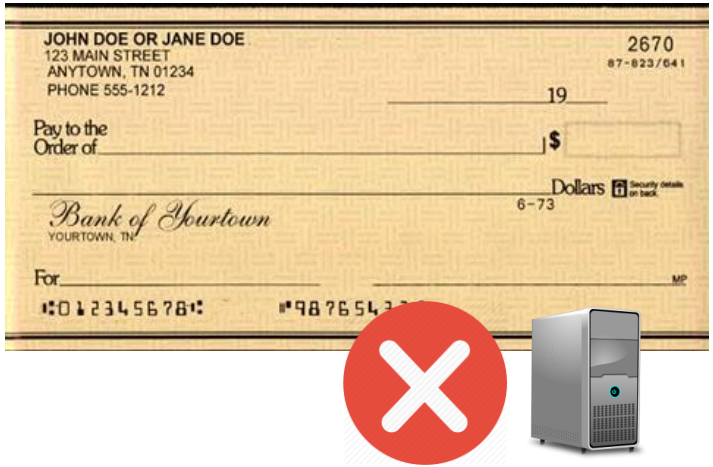


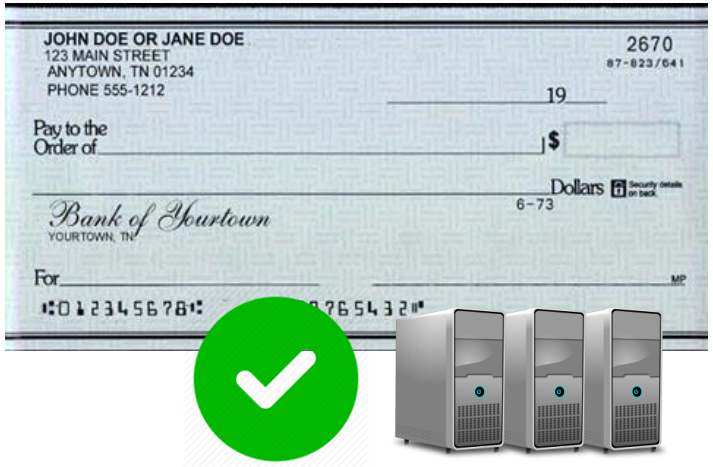


Needed: 3 out of 4 signatures

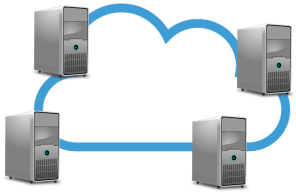
Double-Spending

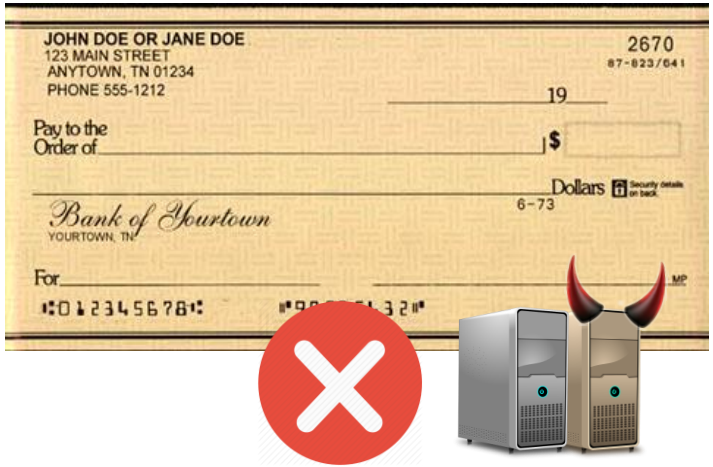


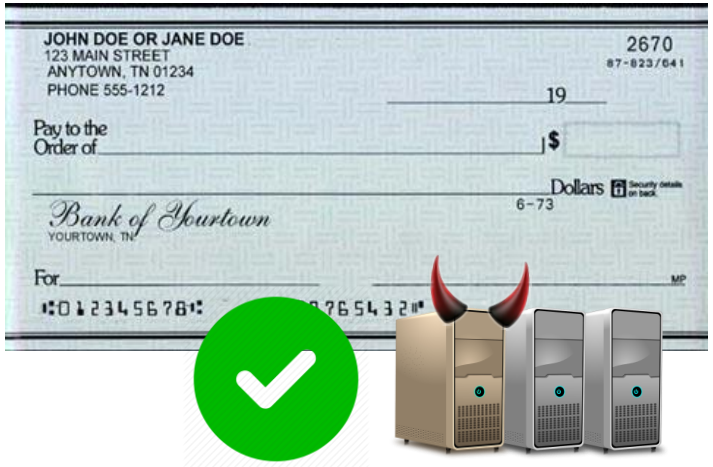




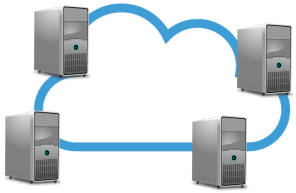
Double-Spending

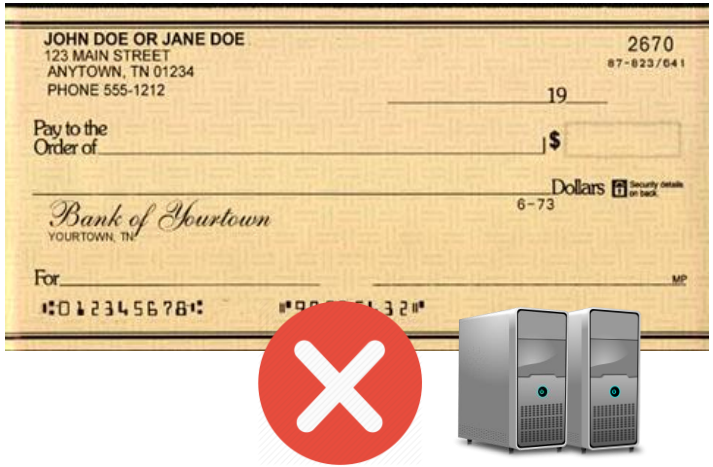


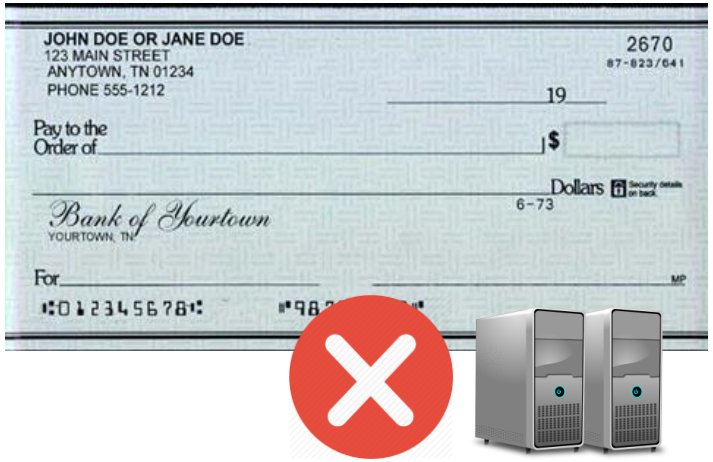




Double-Spending



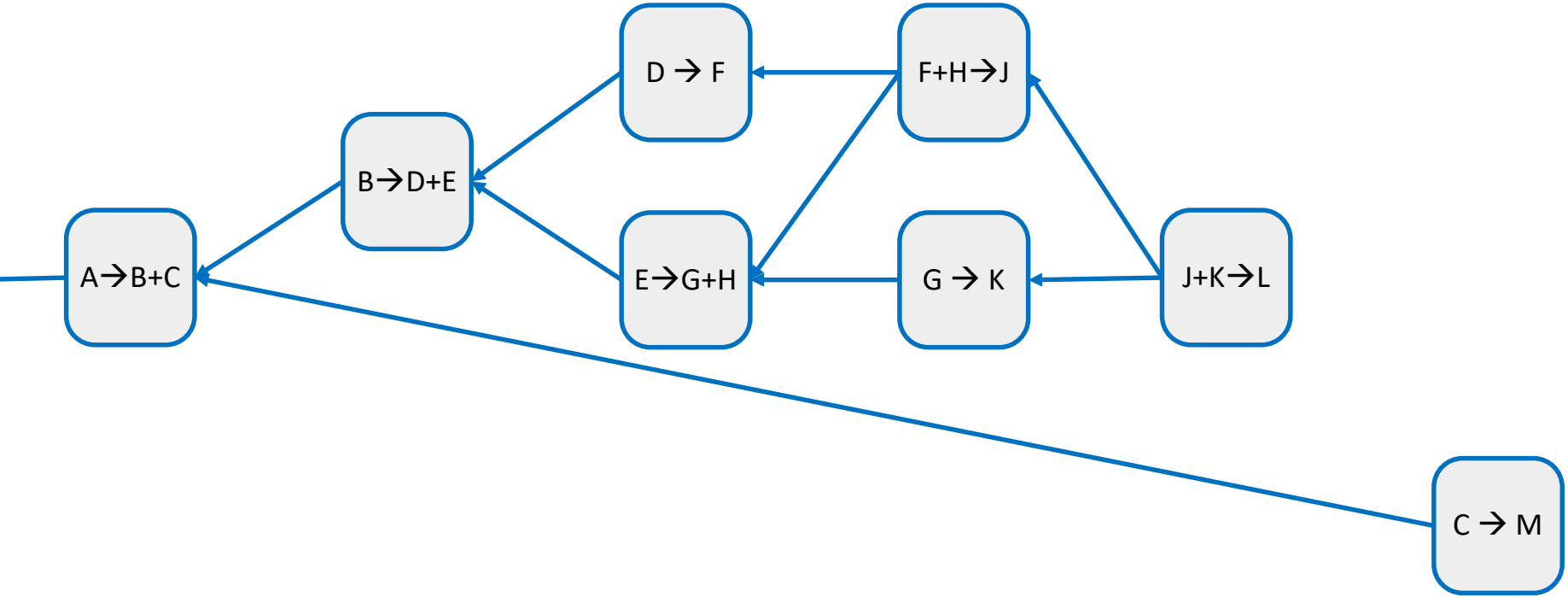




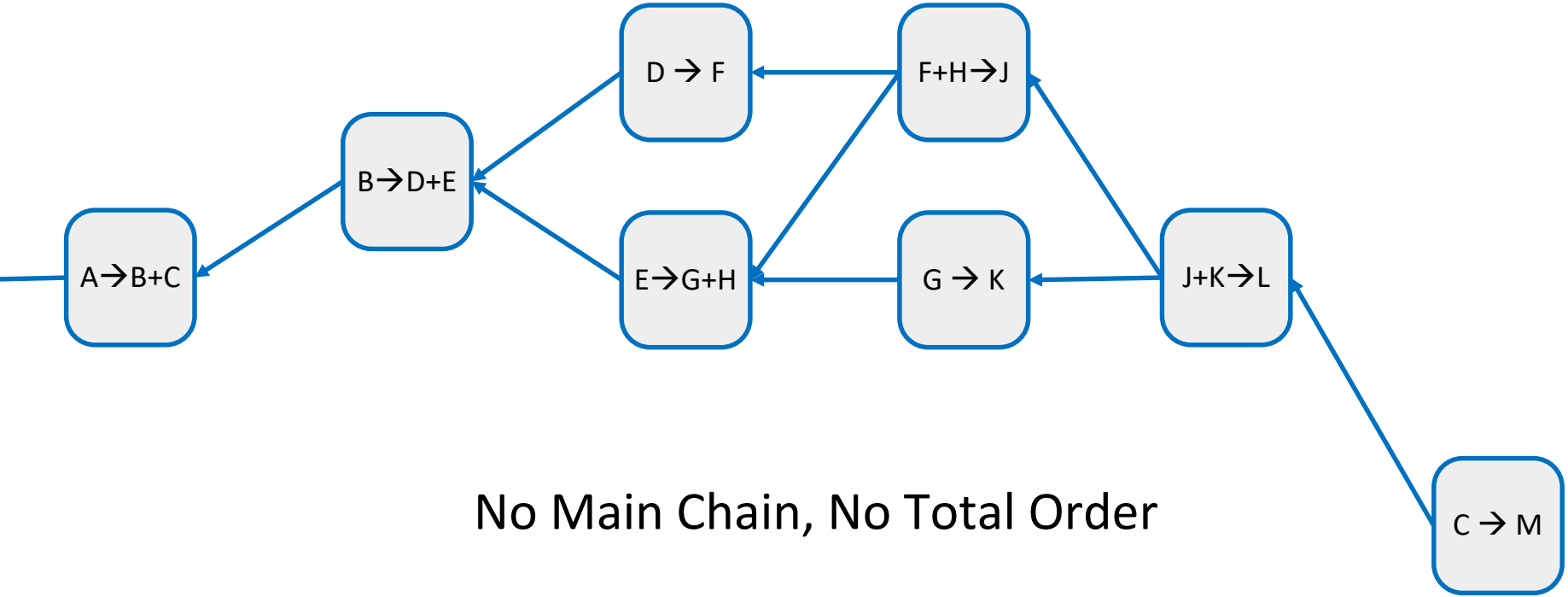
Usual Safety Condition

Less than 1/3 Byzantine

Point to Money Source

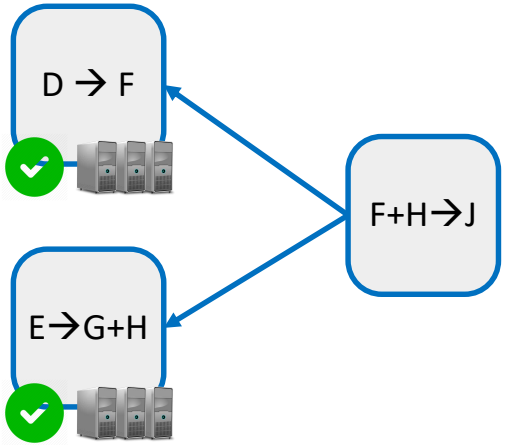


Point To All Transactions!

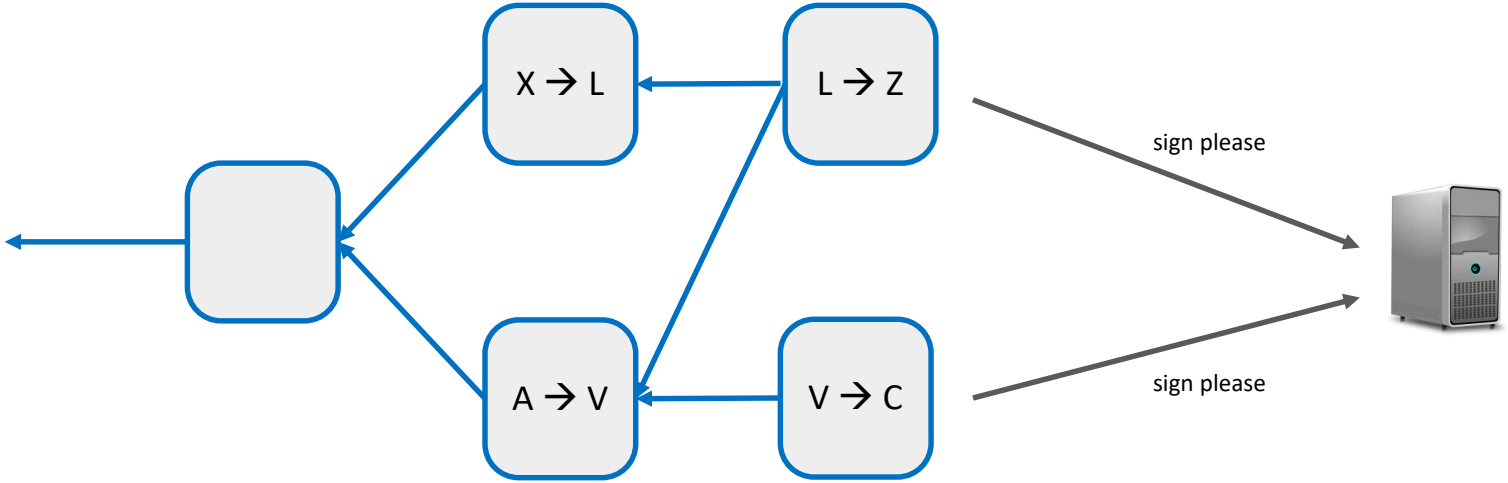


No Main Chain, No Total Order

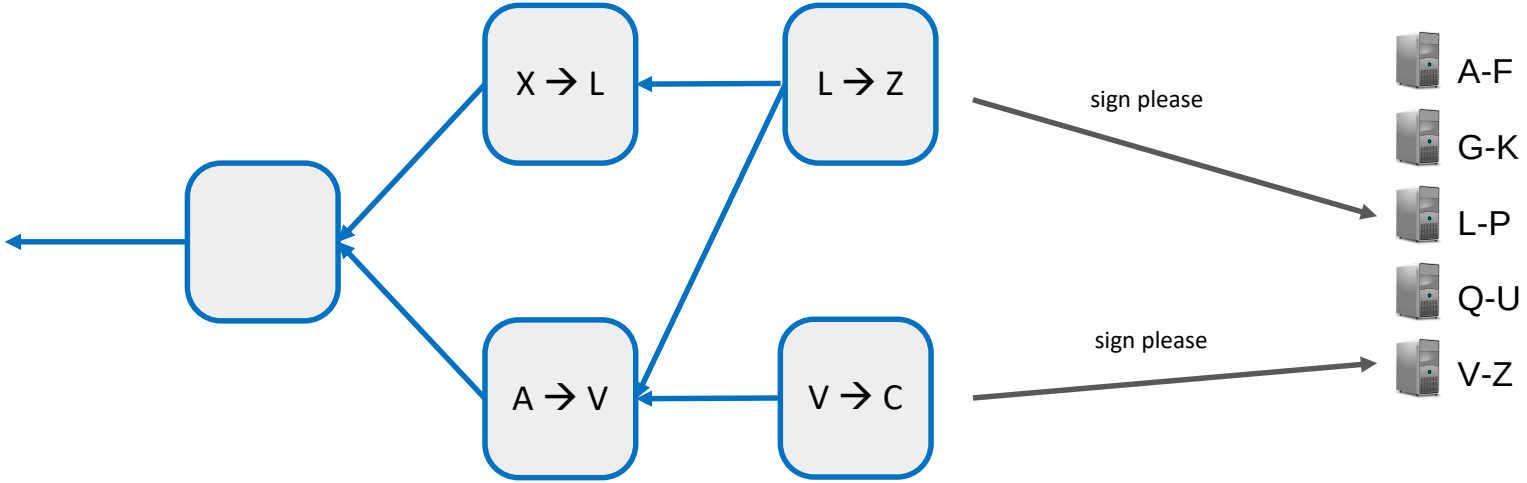
Asynchronous: Without Explicit DAG



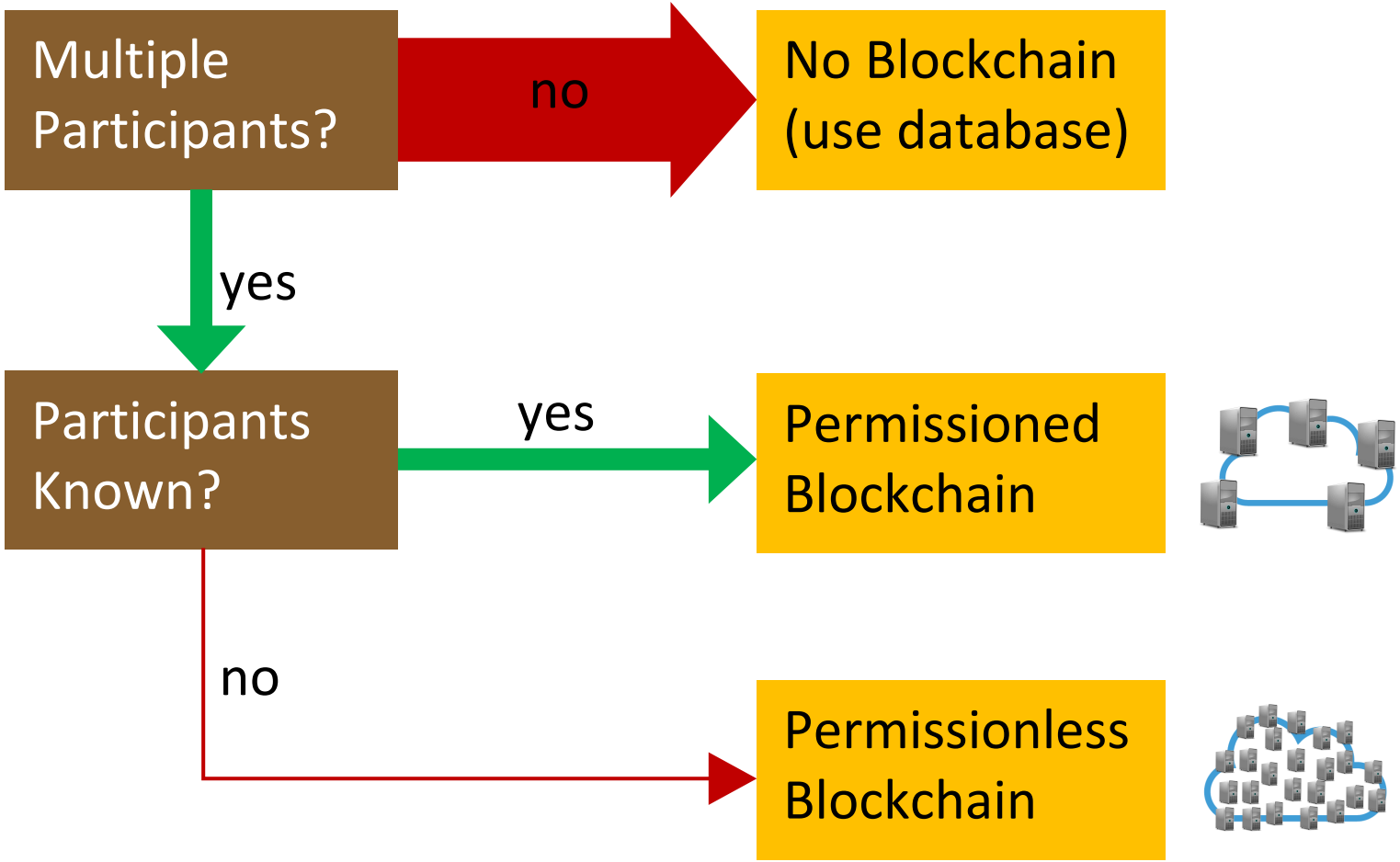
Sharded Signing



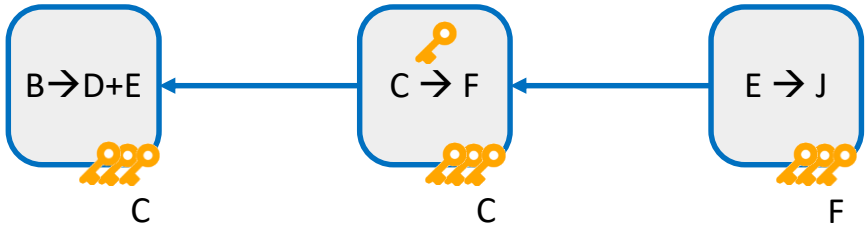
Sharded Signing



Permissionless?

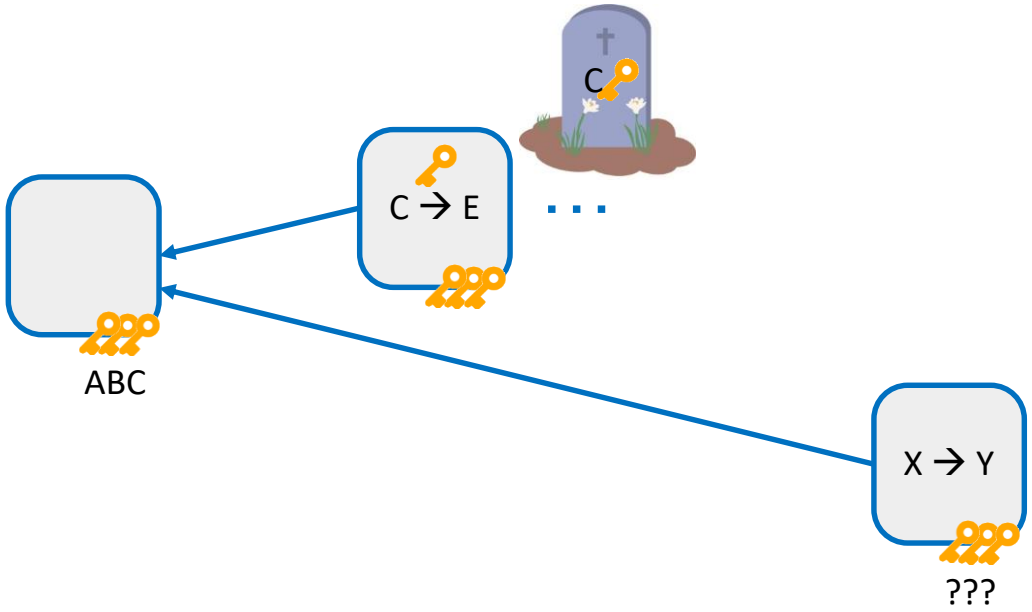

Multiple Participants?
no
No Blockchain (use database)
yes
Participants Known?
yes
Permissioned Blockchain
no
Permissionless Blockchain

1. Transferrable Signing Keys



2. Key Delegation (Pooling)

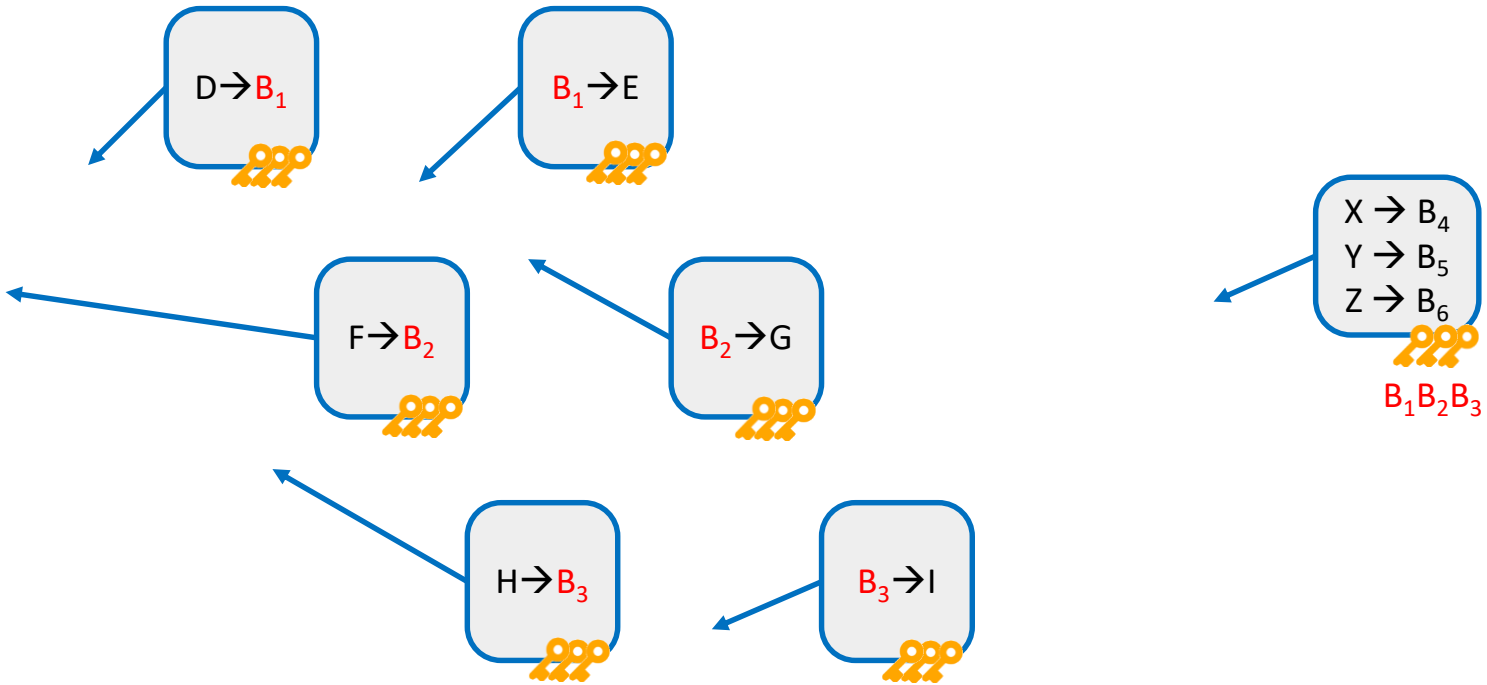
It’s Not So Easy



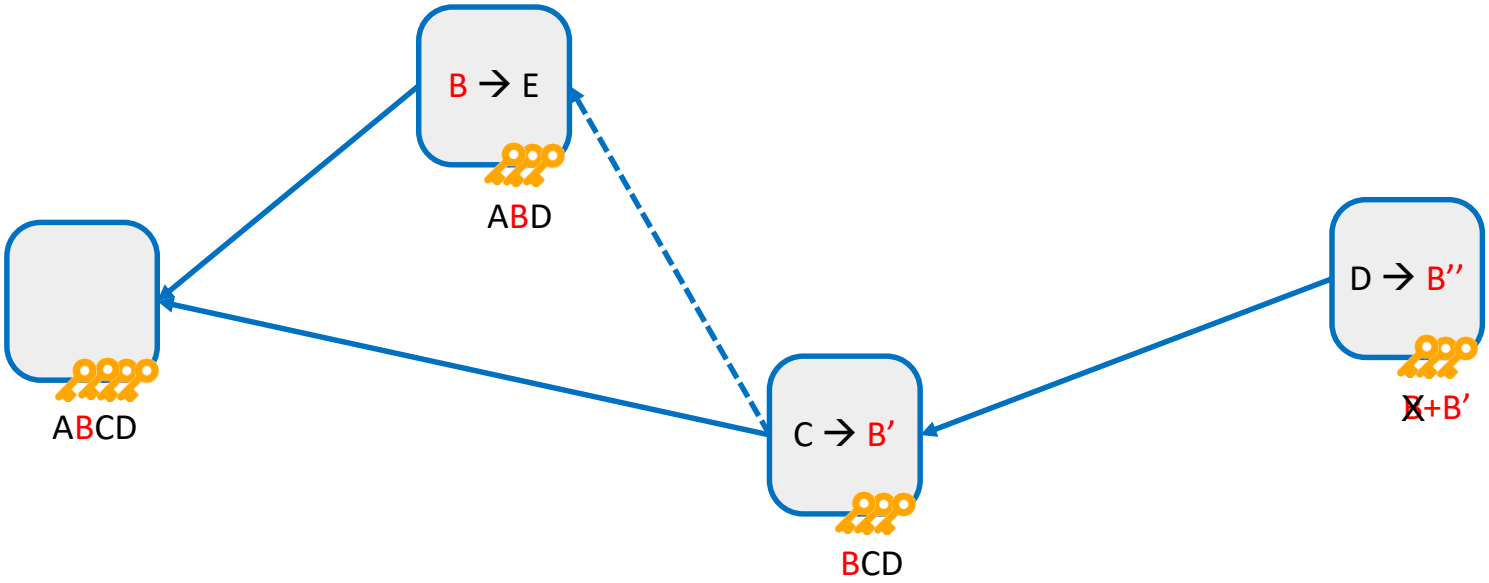
Usual Safety Condition

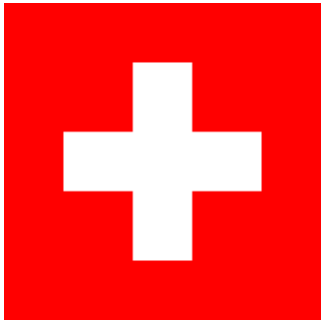
Byzantine $$$ Less Than 1/3 of Stake

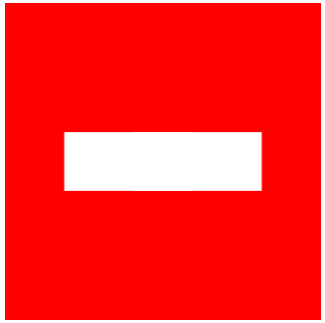
Byzantine Not Burying Keys…



Concrete Example







Asynchronous
Throughput
Finality
Energy (PoS)
Permissionless
Scalable

Smart Contracts?

Summary

Robustness
Fault-Tolerance

Local
Fast

Incentives
Game Theory

Asynchrony
Timing

Security
Privacy

Thank You!

Questions & Comments?


Ene, mene,
eins, zwei, drei,
Bitcoins bringe
mir herbei.
Hash Hash.
@grauhut
BiBi
BlockChain

Persistence

Database

↓

Immutable

↓

Provable

Fault-Tolerance

Correct

↓

Crash

↓

Byzantine

Latency

1 hour

↓

1 minute

↓

1 second

Throughput

10 tx/s

↓

10k tx/s

↓

10m tx/s

Replication

main+backup

↓

some nodes

↓

1000 nodes

Energy

Proof-of-Work

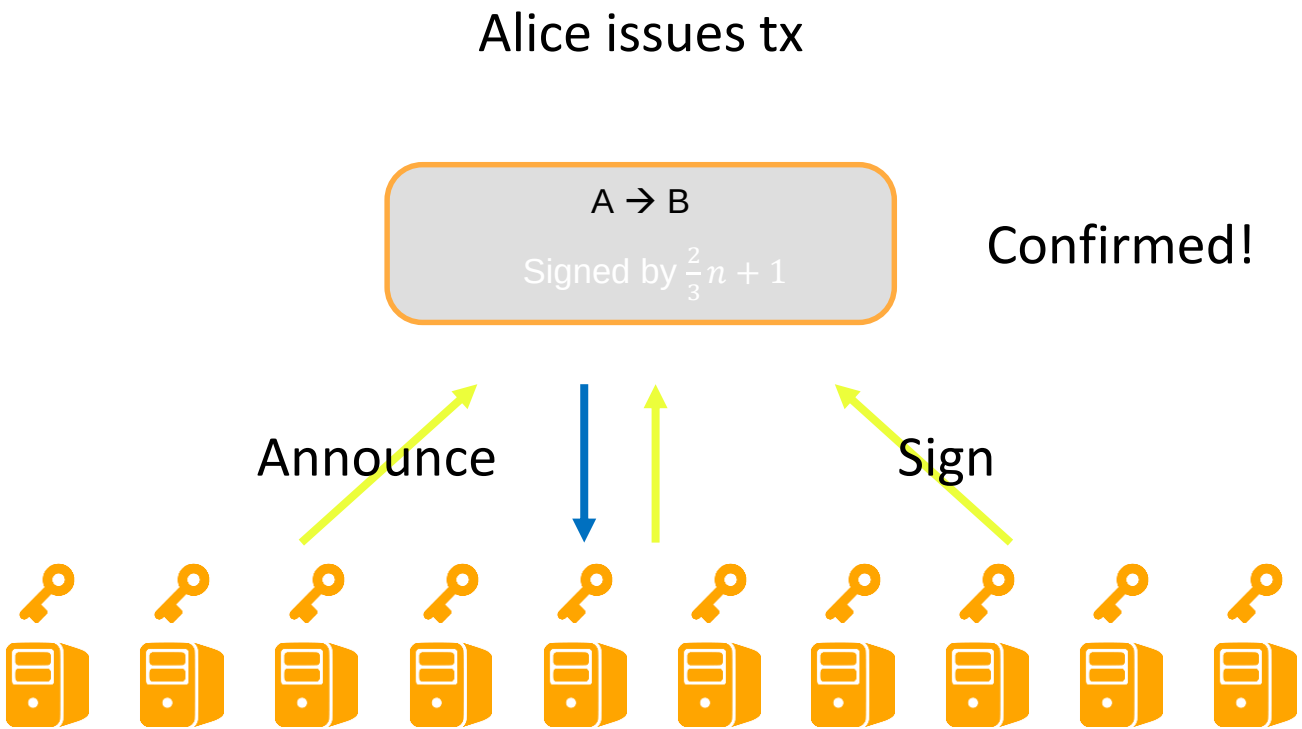
↓

Proof-of-Stake

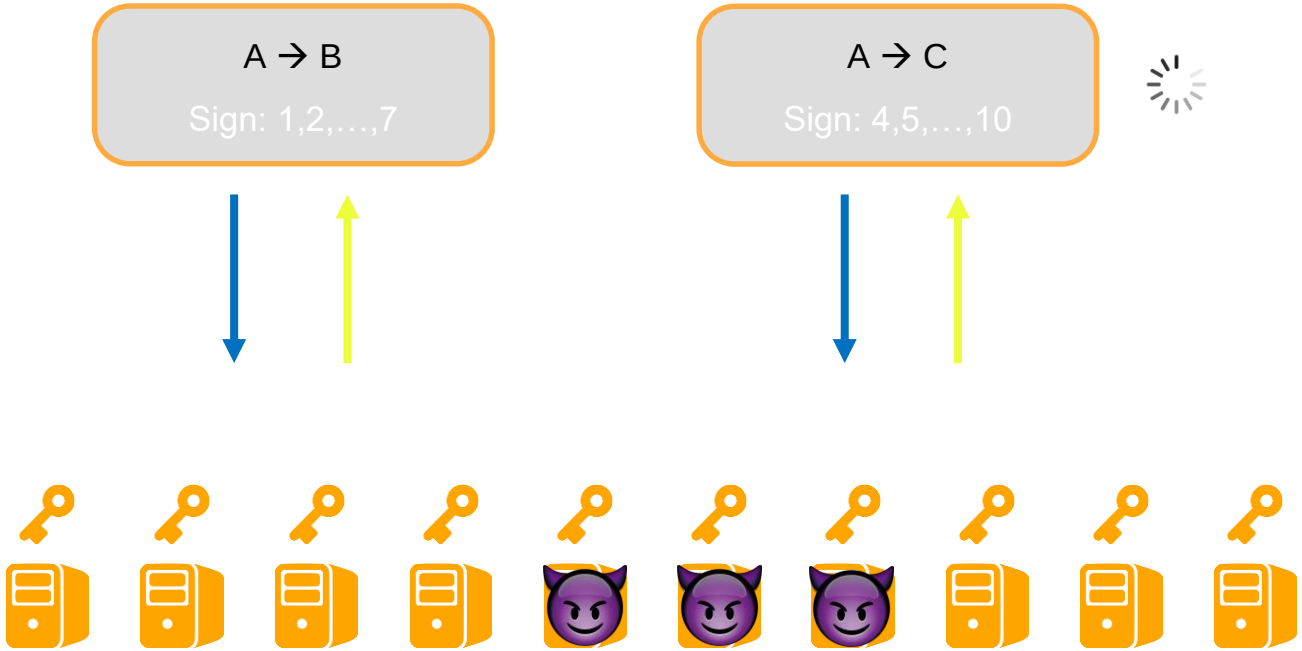
↓

Permissioned

Simple confirmation



No double-spending



No double-spending

A → B

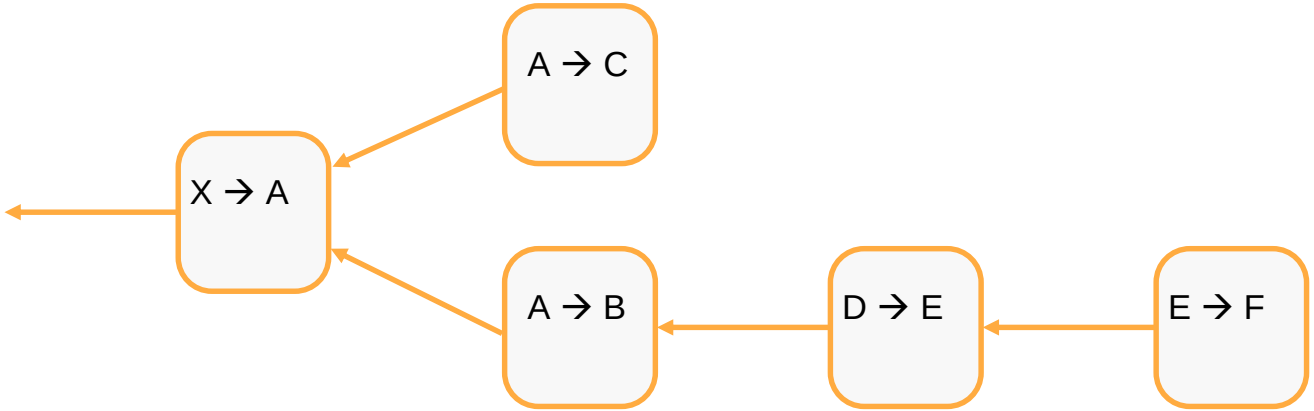
Sign: 1,2,3,4,5

A → C

Sign: 6,7,8,9,10

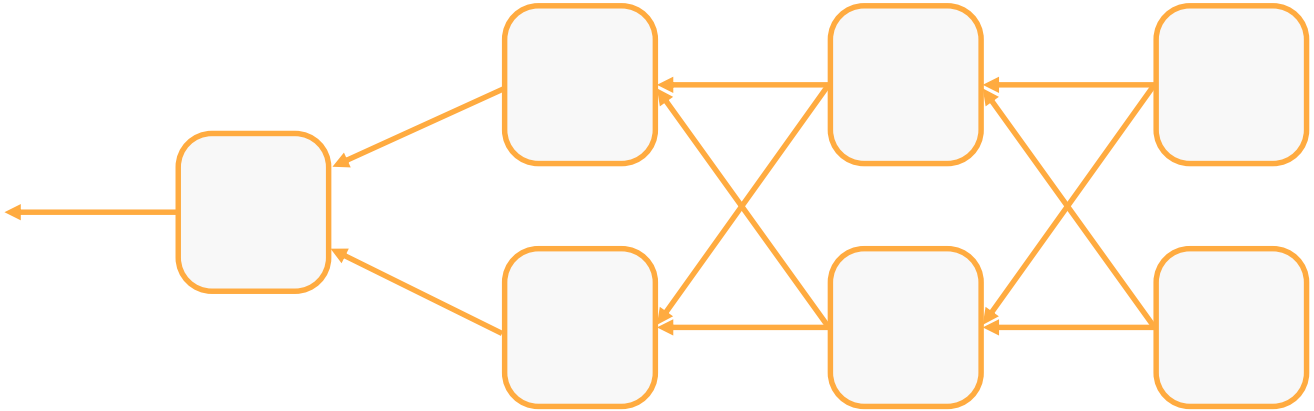
A →

Q: But if we have two unconfirmed alternatives, how to progress?



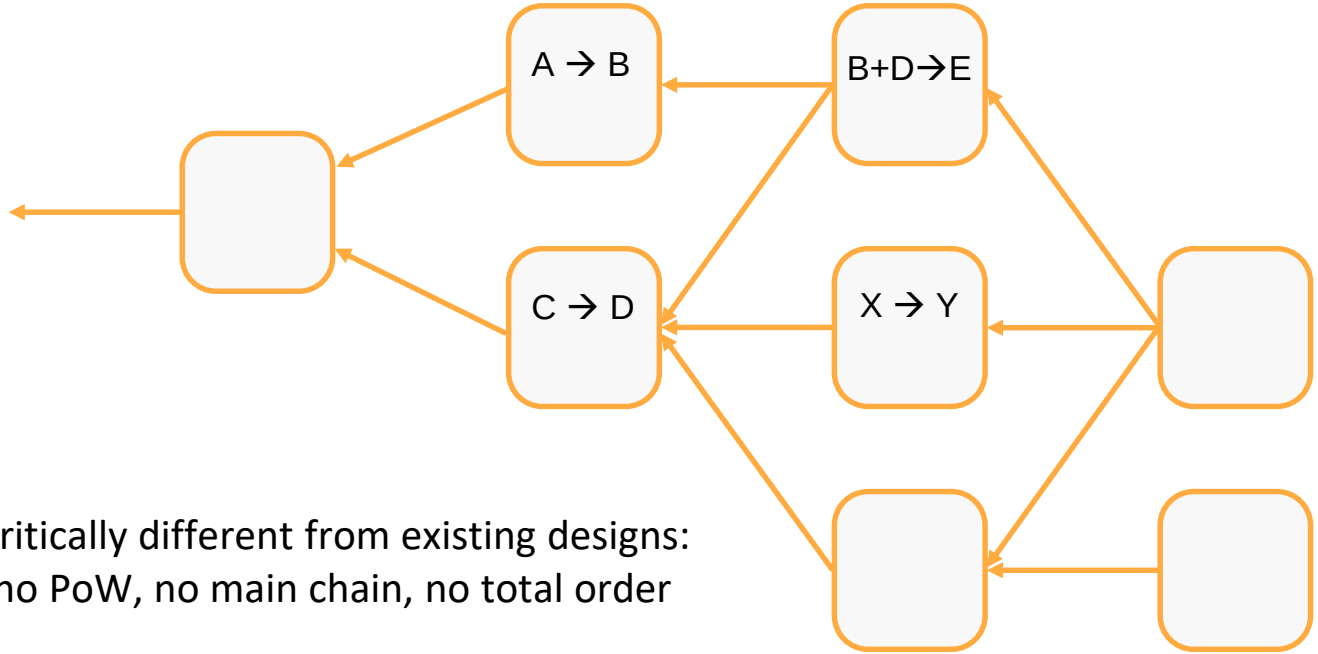
A: Not all transactions need to be confirmed, just carry on.

Q: So there will be forks, even by chance.
Where do I attach the next transaction?



A: There’s no need for a single history/chain,
attach everywhere.

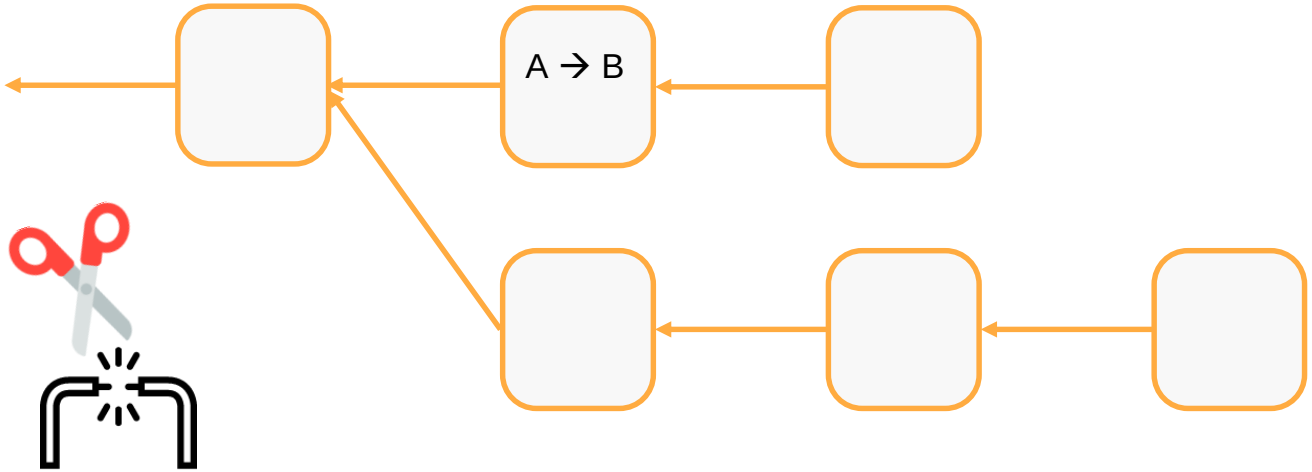
Directed Acyclic Graph



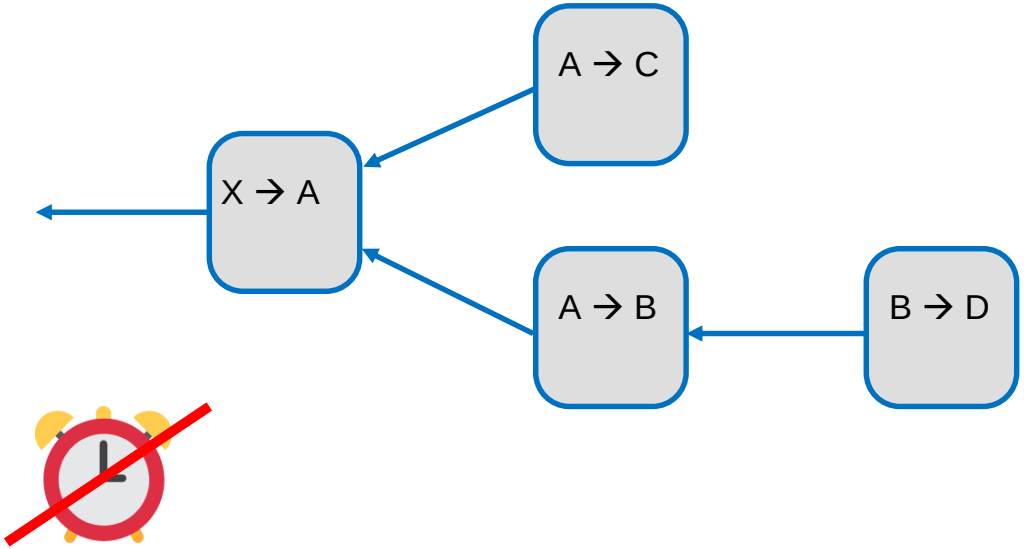
Critically different from existing designs:
no PoW, no main chain, no total order

What about time?

Bitcoin

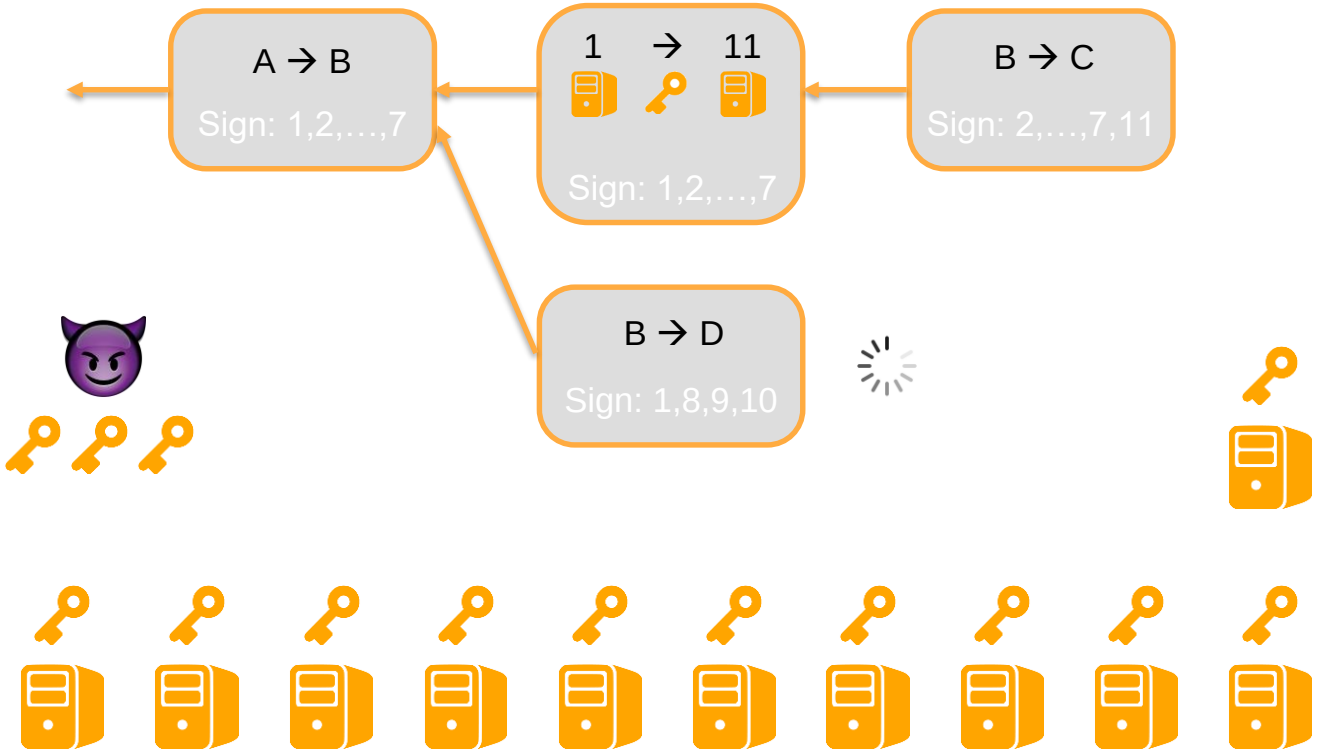


Us: fully asynchronous

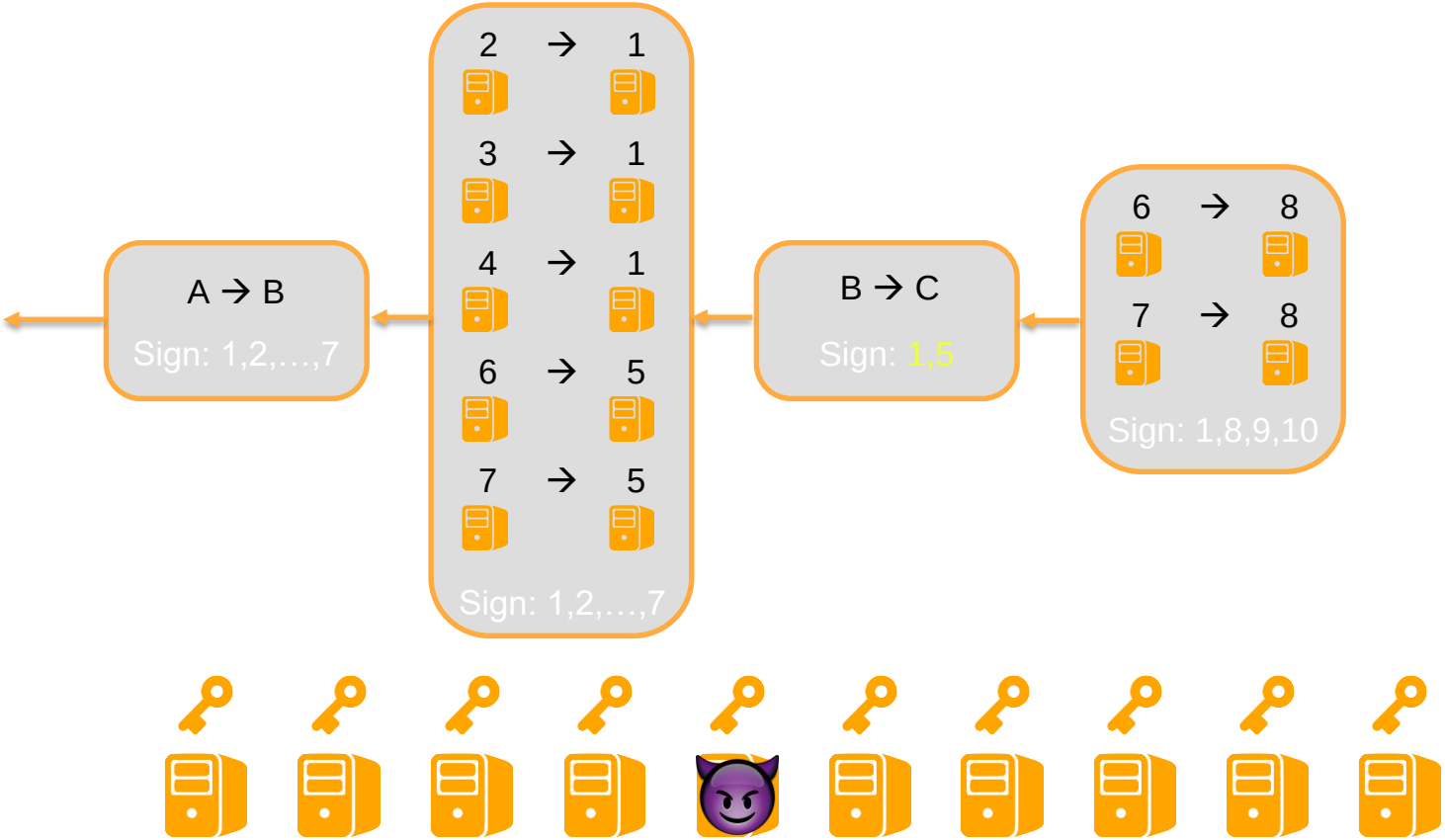


Is it a permissioned blockchain?

Keys are transferrable



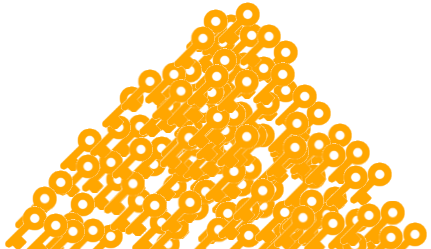
Key delegation



Proof of Stake

1 token = 10000 🔑

~ ฿ mining pools



Delegated to verifiers:

 = 3261768 t

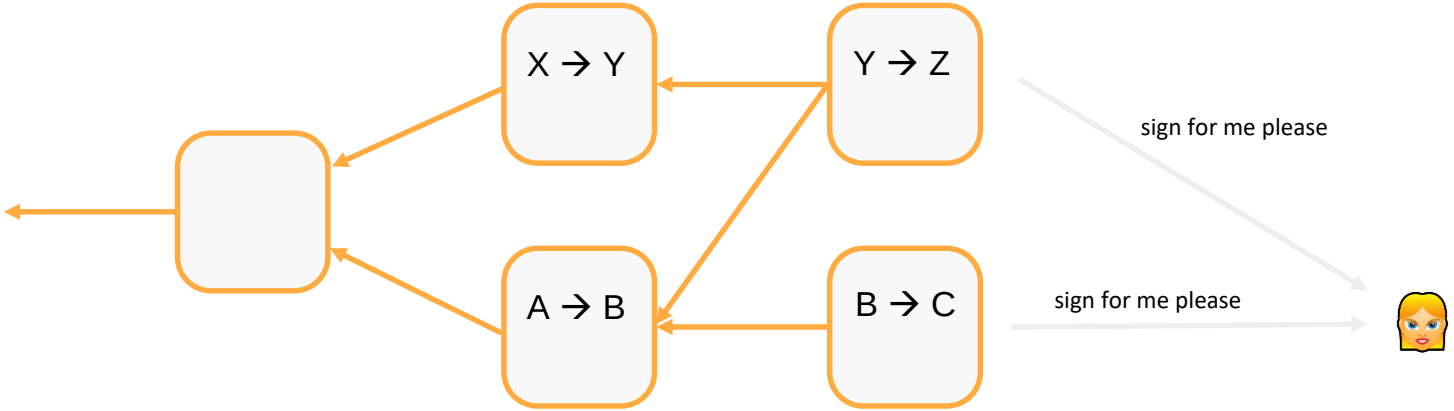
 = 2893498 t

 = 947348 t

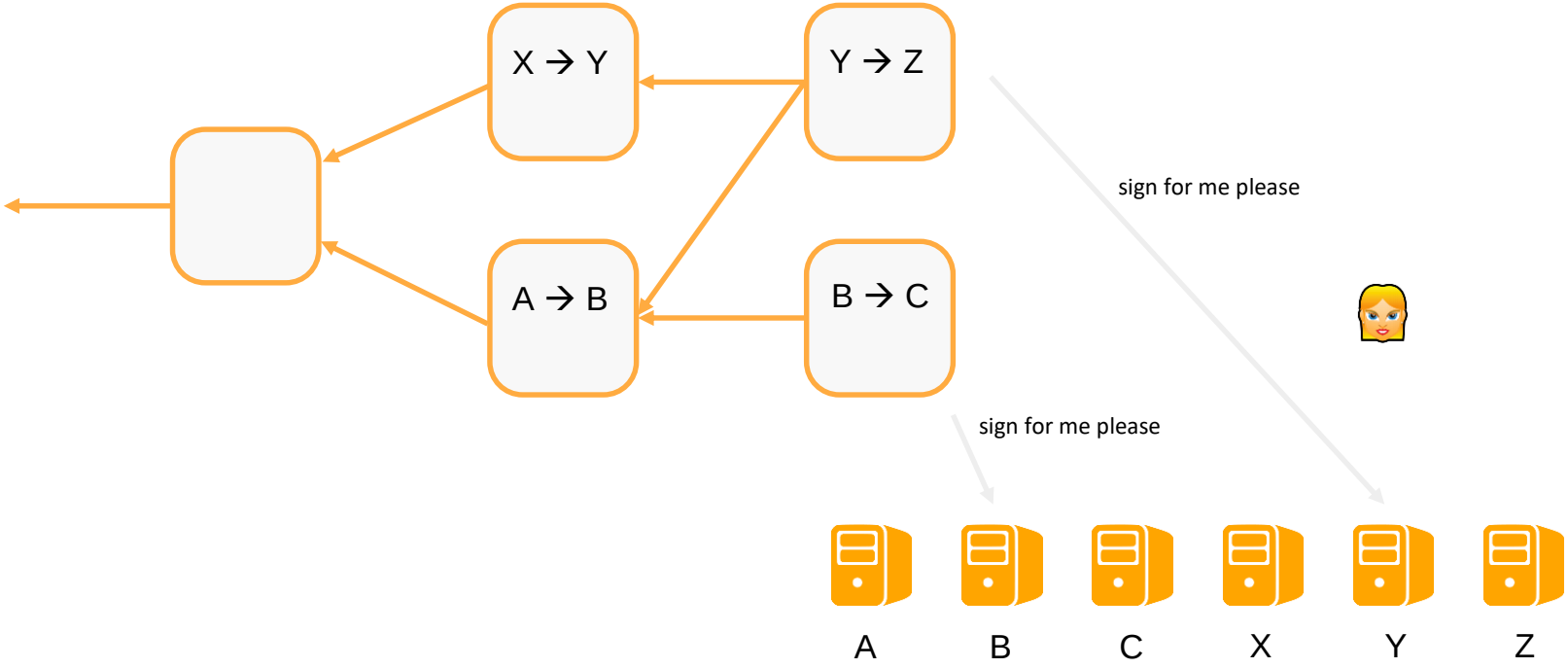
 = 897634 t

...

Parallel processing



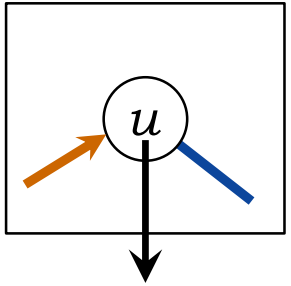
Parallel processing



Best solution – maximizing a node's payoff

Reduction to *Maximum Independent Set*

Node Gadget



indicator bank

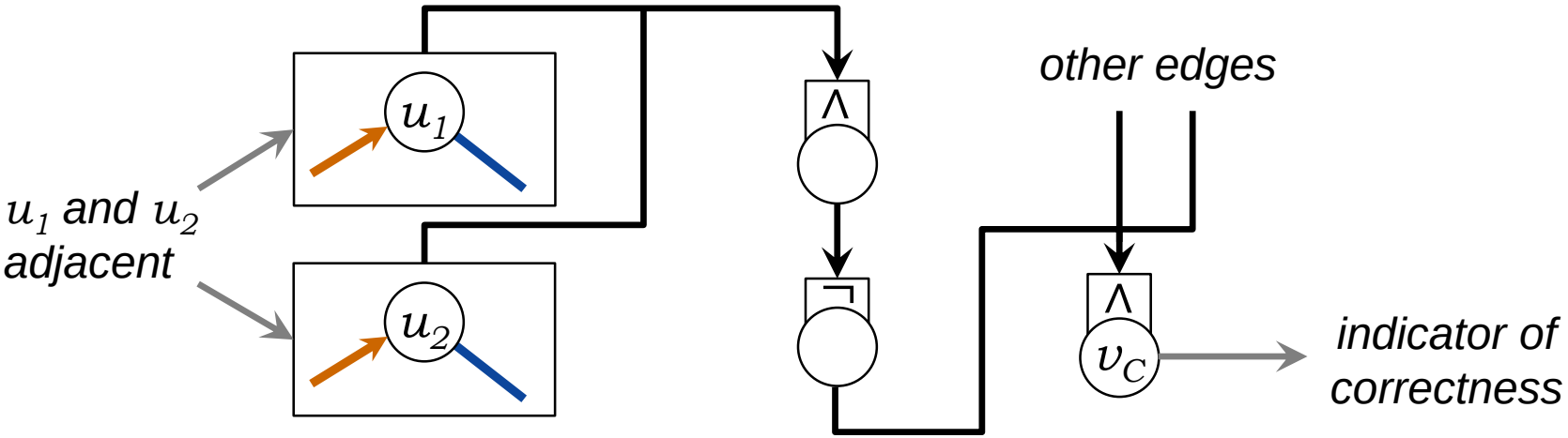
$$r_u = 0 \quad or \quad r_u = 1$$

$$\Updownarrow \qquad\qquad \Updownarrow$$

$$u \notin S \qquad\qquad u \in S$$

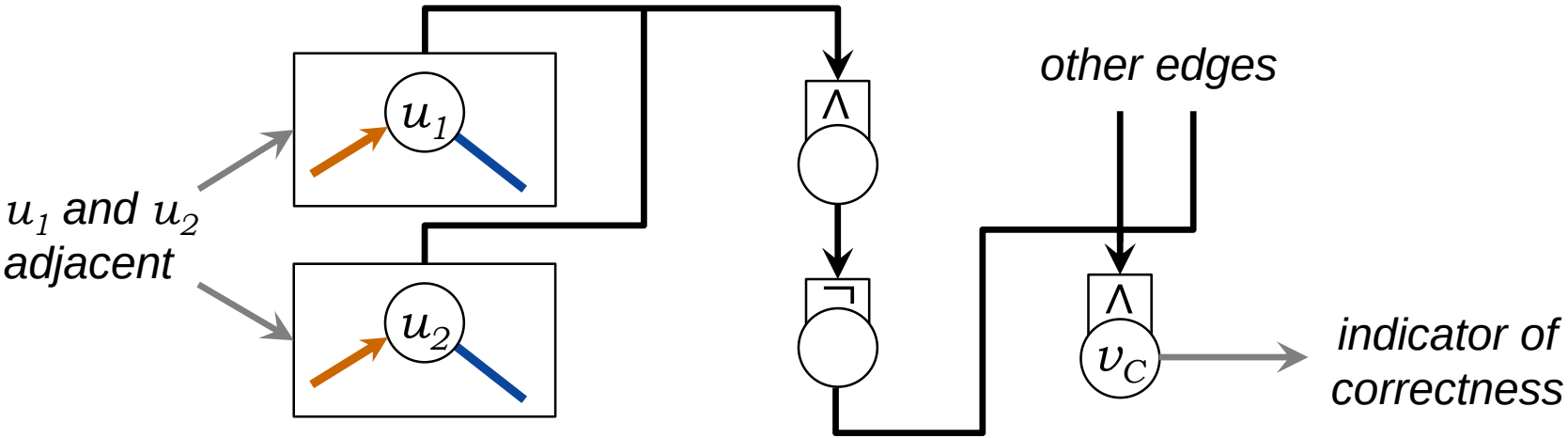
Best solution – maximizing a node's payoff

Reduction to *Maximum Independent Set*



Best solution – maximizing a node's payoff

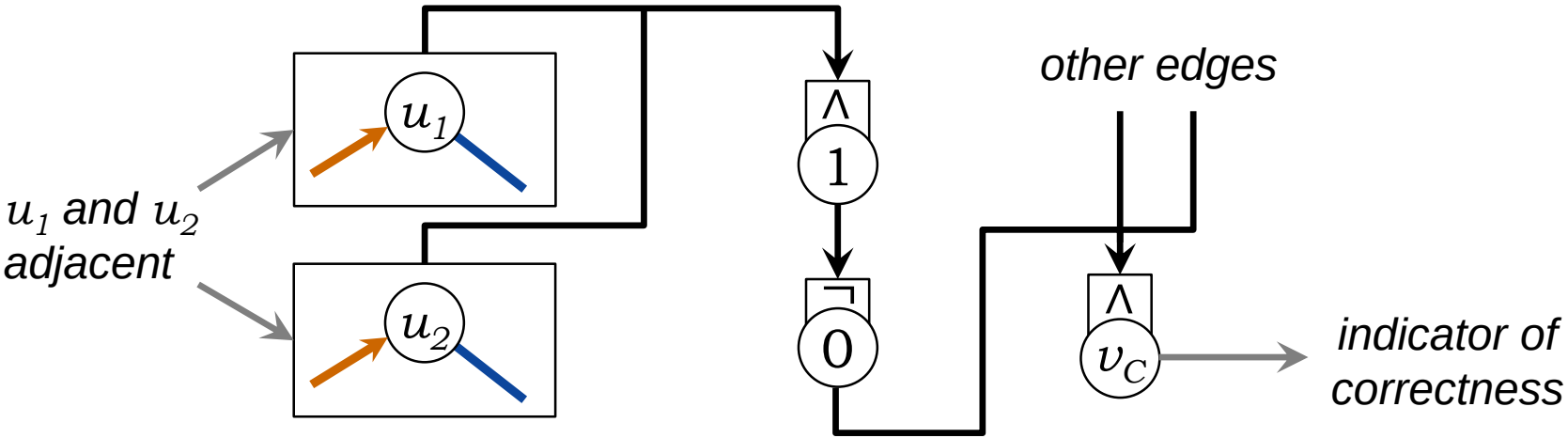
Reduction to *Maximum Independent Set*



$$u_1, u_2 \in S$$

Best solution – maximizing a node's payoff

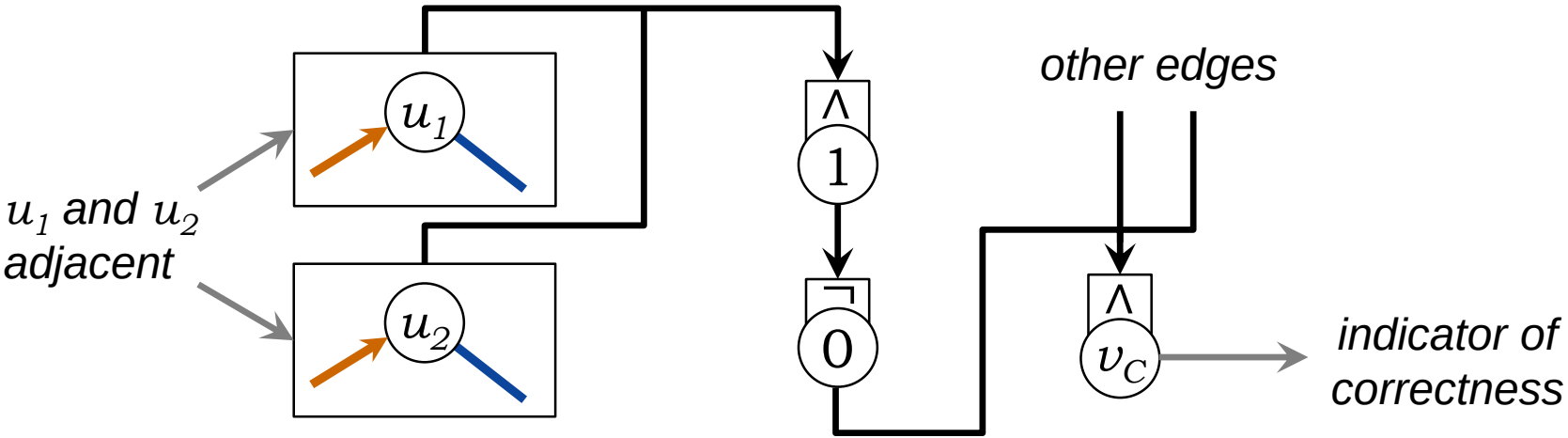
Reduction to *Maximum Independent Set*



$$u_1, u_2 \in S$$

Best solution – maximizing a node's payoff

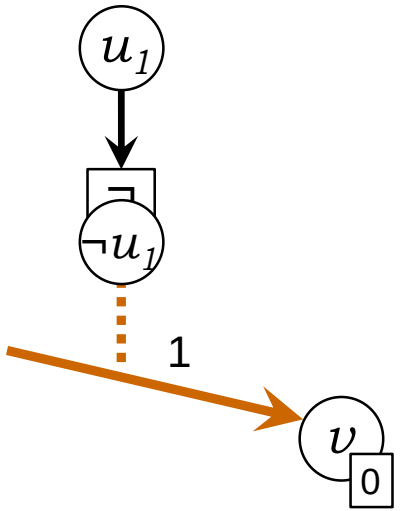
Reduction to *Maximum Independent Set*



$$u_1, u_2 \in S \quad \Rightarrow \quad r_{v_C} = 0$$

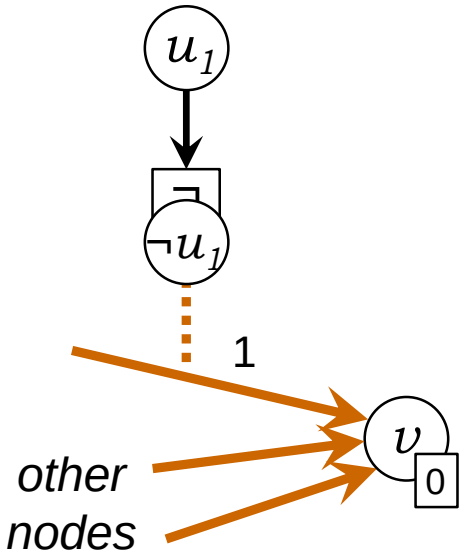
Best solution − maximizing a node's payoff

Reduction to *Maximum Independent Set*



Best solution − maximizing a node's payoff

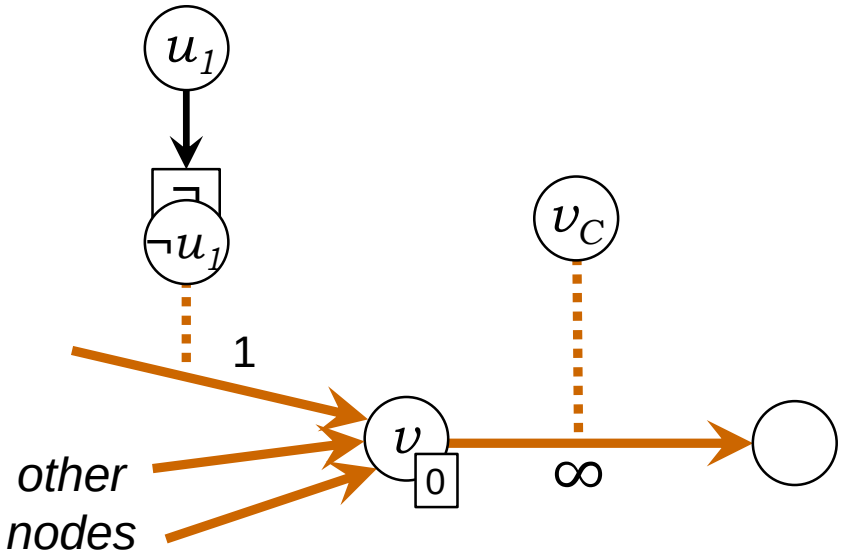
Reduction to *Maximum Independent Set*



$$a_v = \#\text{ of nodes in } S$$

Best solution – maximizing a node's payoff

Reduction to *Maximum Independent Set*



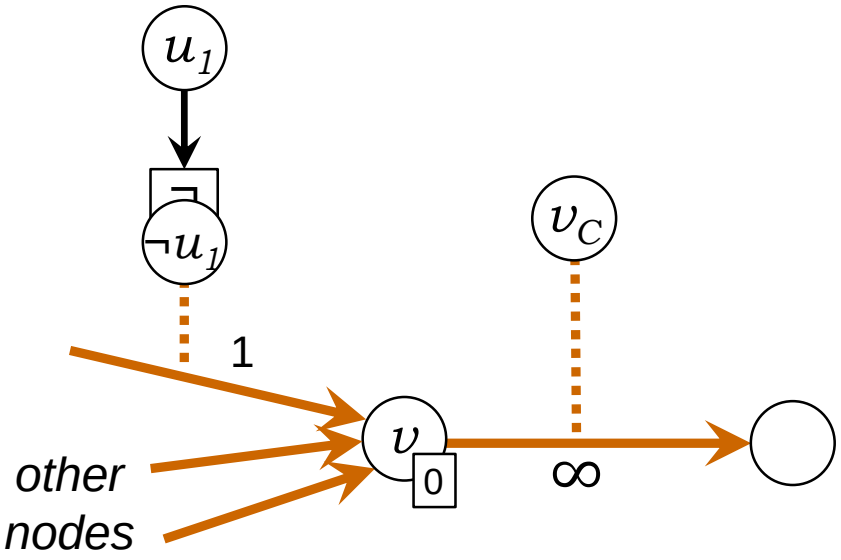
$$a_v = \#\text{ of nodes in } S$$

$$\downarrow$$

but 0 if not independent!

Best solution – maximizing a node's payoff

Reduction to *Maximum Independent Set*



$$a_v = \#\text{ of nodes in } S$$

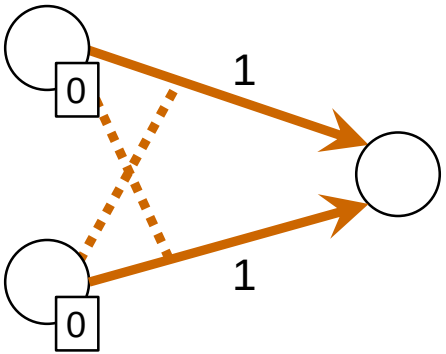
$$\downarrow$$

but 0 if not independent!

Max. independent set $\longleftrightarrow$ Max. payoff

Computing with financial networks

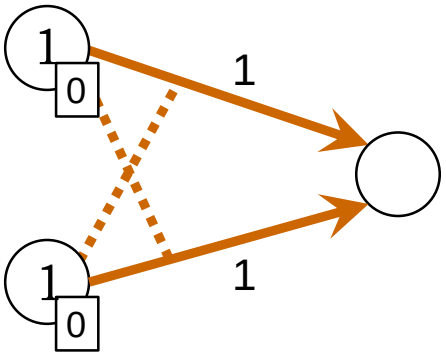
Symbols on tape



Bit gadget

Computing with financial networks

Symbols on tape

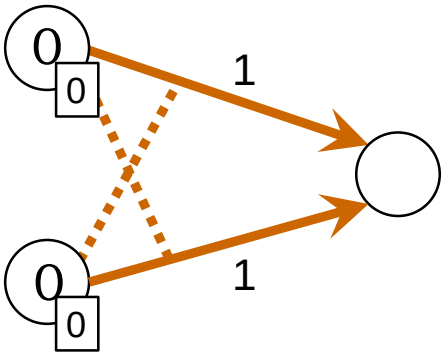


Bit gadget

both (1,1) and (0,0) are stable states

Computing with financial networks

Symbols on tape

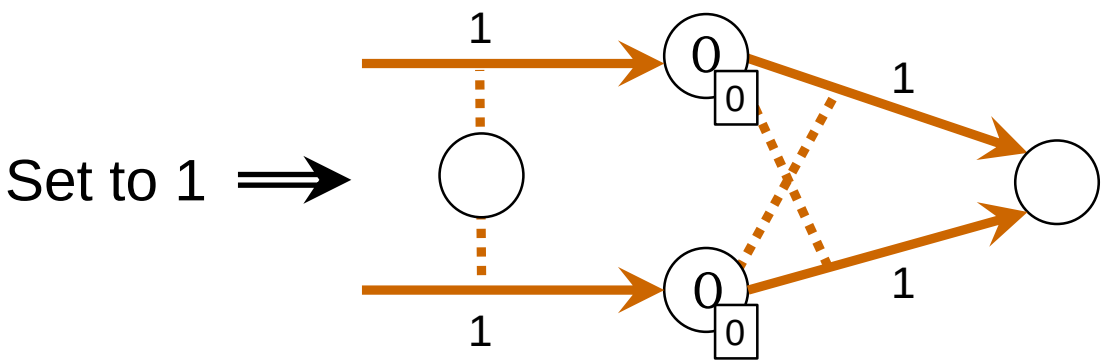


Bit gadget

both (1,1) and (0,0) are stable states

Computing with financial networks

Symbols on tape

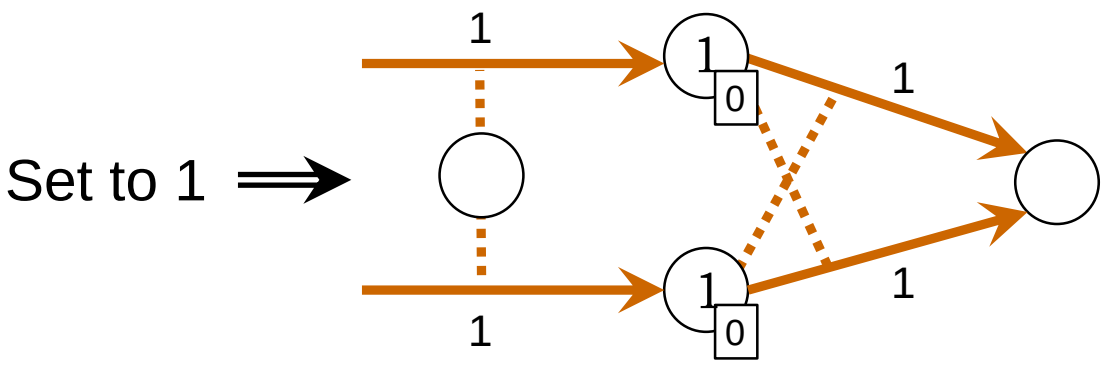


Bit gadget

both (1,1) and (0,0) are stable states

Computing with financial networks

Symbols on tape

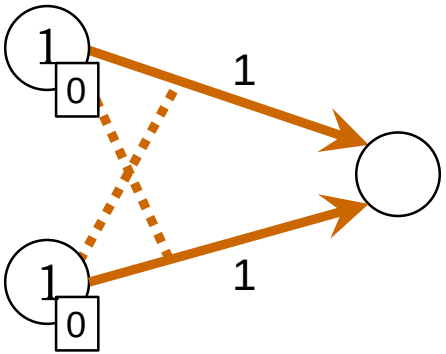


Bit gadget

both (1,1) and (0,0) are stable states

Computing with financial networks

Symbols on tape

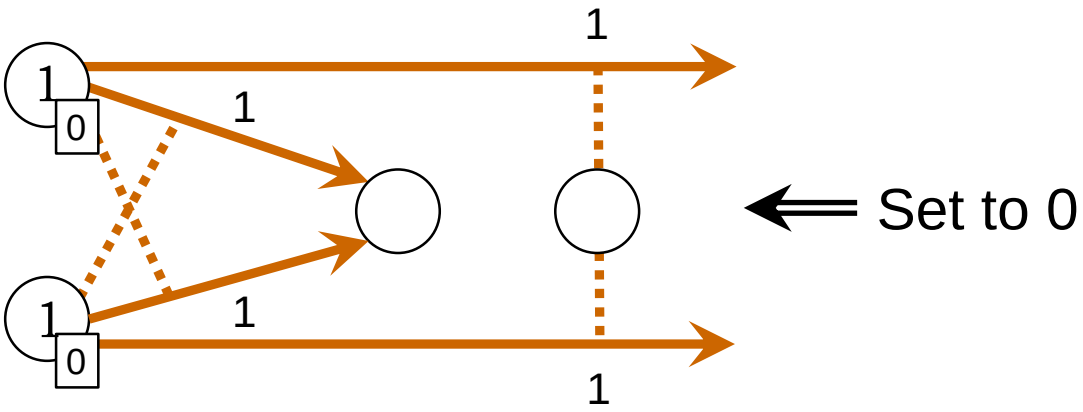


Bit gadget

both (1,1) and (0,0) are stable states

Computing with financial networks

Symbols on tape

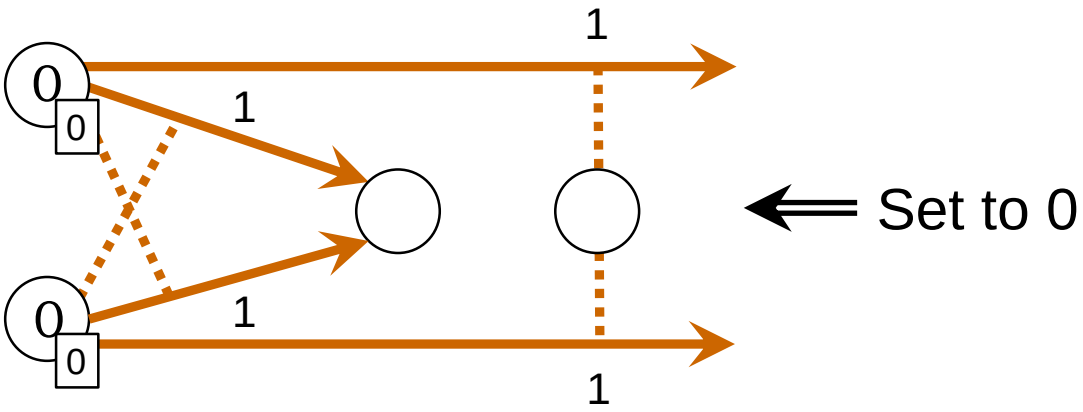


Bit gadget

both (1,1) and (0,0) are stable states

Computing with financial networks

Symbols on tape

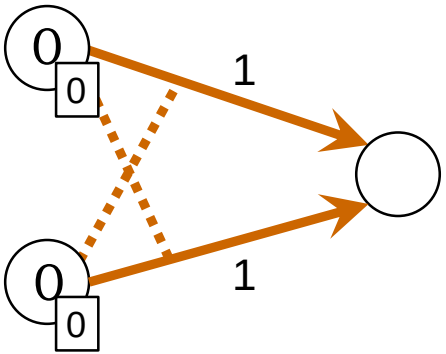


Bit gadget

both (1,1) and (0,0) are stable states

Computing with financial networks

Symbols on tape



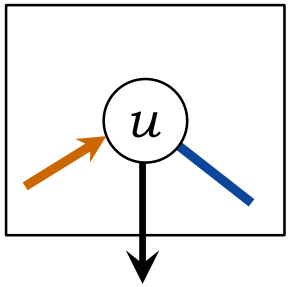
Bit gadget

both (1,1) and (0,0) are stable states

Computing with financial networks

Finite automaton

Current state

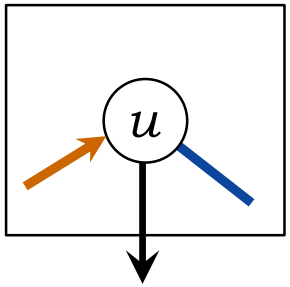


indicator bank

Computing with financial networks

Finite automaton

Current state



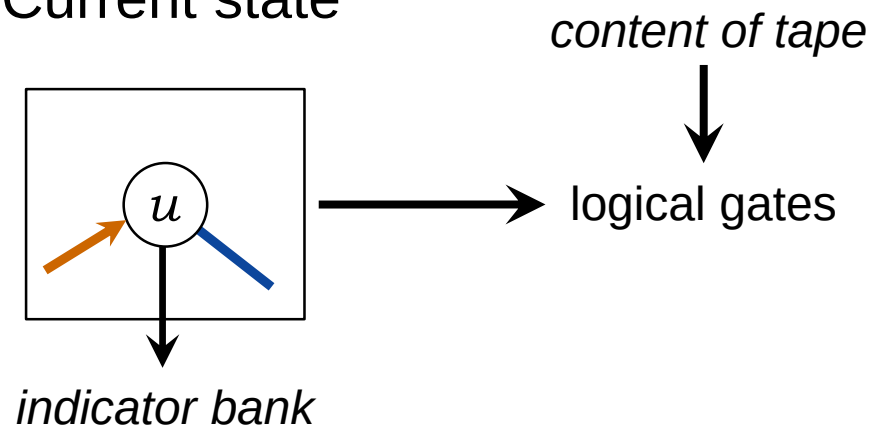
indicator bank

$r_u = 0 \quad \Leftrightarrow$ this is the current state

Computing with financial networks

Finite automaton

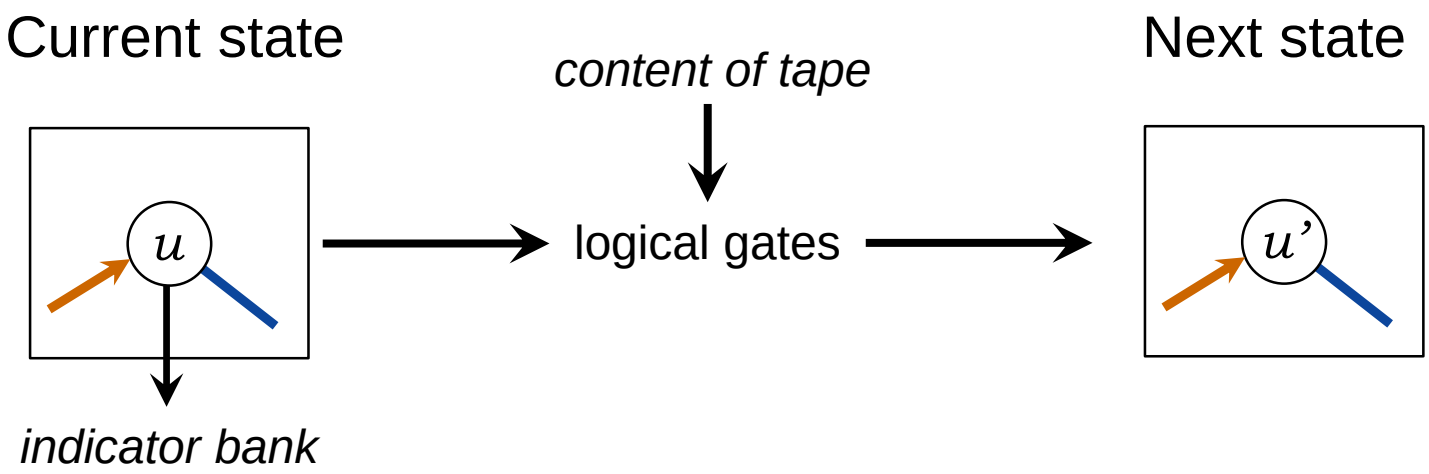
Current state



$r_u = 0 \quad \Leftrightarrow$ this is the current state

Computing with financial networks

Finite automaton



$r_u = 0 \quad \Leftrightarrow$ this is the current state