Cross-Chain Deals and Adversarial Commerce

SOSP 2019 Diversity Workshop

October 2019

Liuba Shrira
Brandeis University
and Algorand

Cross-chain Deals and Adversarial Commerce

Maurice Herlihy
Brown University
mph@cs.brown.edu

Barbara Liskov
MIT CSAIL
liskov@csail.mit.edu

Liuba Shrira
Brandeis University
liuba@brandeis.edu

Your speaker

ABSTRACT

Modern distributed data management systems face a new challenge: how can autonomous, mutually-distrusting parties cooperate safely and effectively? Addressing this challenge brings up questions familiar from classical distributed systems: how to combine multiple steps into a single atomic action, how to recover from failures, and how to synchronize concurrent access to data. Nevertheless, each c
requires rethinking when participants are au
potentially adversarial.

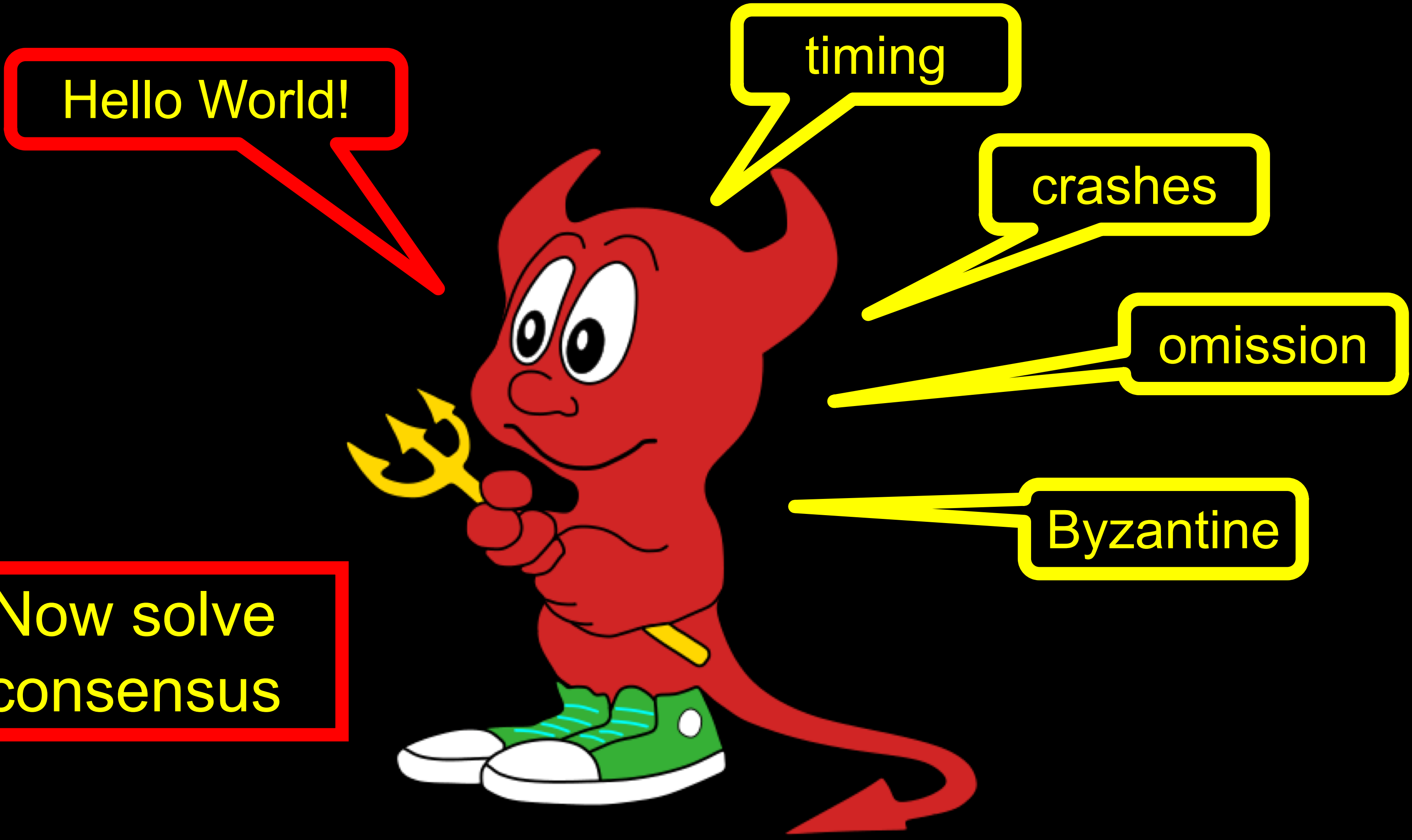
We propose the notion of a cro
deal, a new way
to structure complex distributed
assets in an adversarial setti
transactions, but are
modate the decentralized
describe novel safety

VLDB 2020, to appear

from, classical atomic transactions. In particular, the classical notions of correctness for atomic transactions must be
rethought.

Classical atomicity means that a transaction's effects tak
place everywhere or nowhere. This notion of atomicity ca
not be guaranteed when parties are potentially malicio
the best one can do is to ensure that honest parties can
be cheated. Moreover, classical transactions often priori
liveness, allowing, for example, commit pr
k [41]. For cross-chain commerce, how
es have been relied upon to ensure tha
ck another into locking up assets forev
even for a long time.

guarantees that concurrent trans
ways. Isolation is ty
such as serializability or s
perties are poorly suited t
consistency, where mutually-untrusting parties
chain commerce, cautious interactions to set up and
takes the form of
one party



Now solve consensus

Classical Adversary

Привет мир!

你好，世界！

שלום עולם!

سلام دنيا!

Side-channels

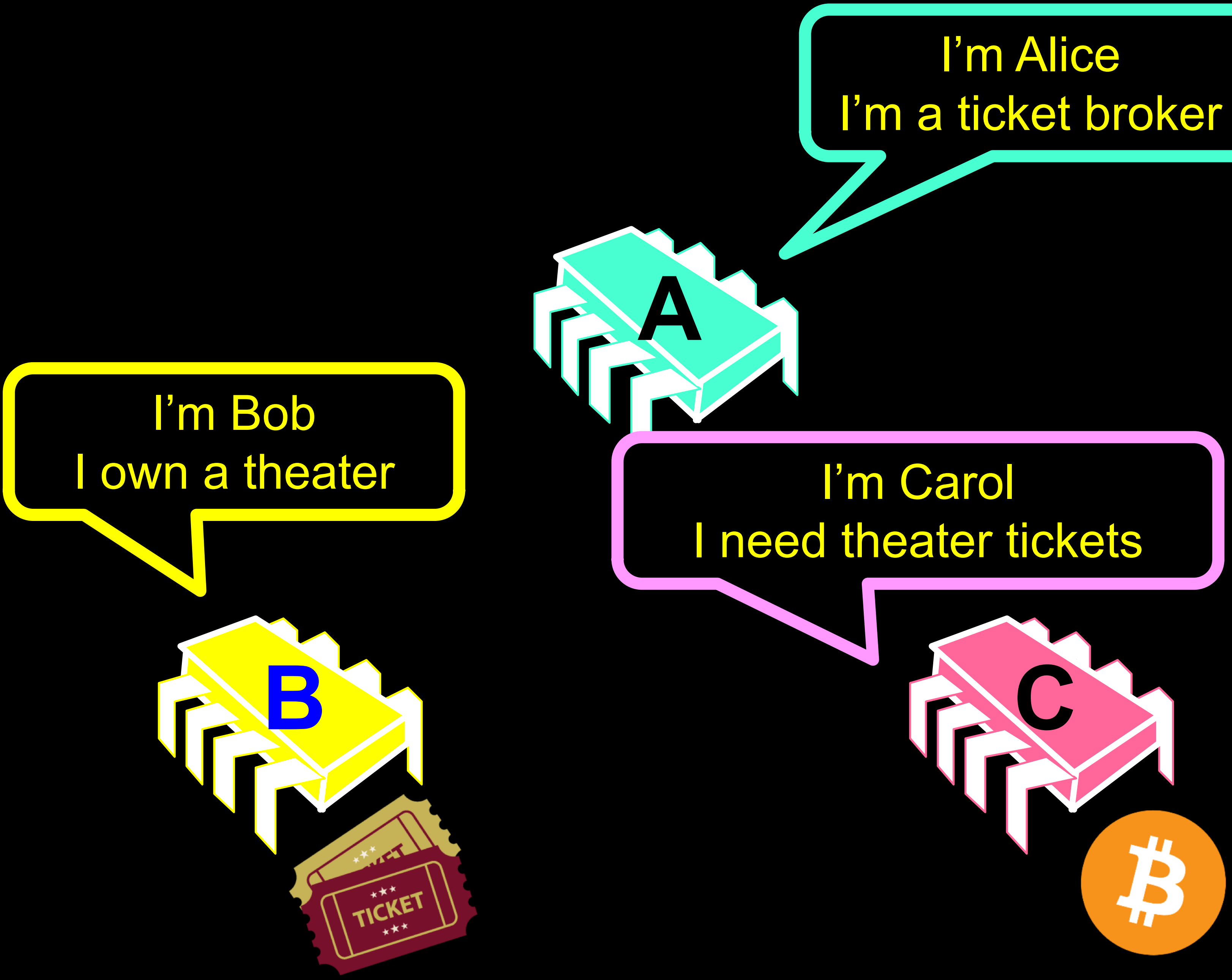
rootkits

Eclipse, 51%, re-enrancy …

zero-day

Now hold a free and fair election

Modern Adversary

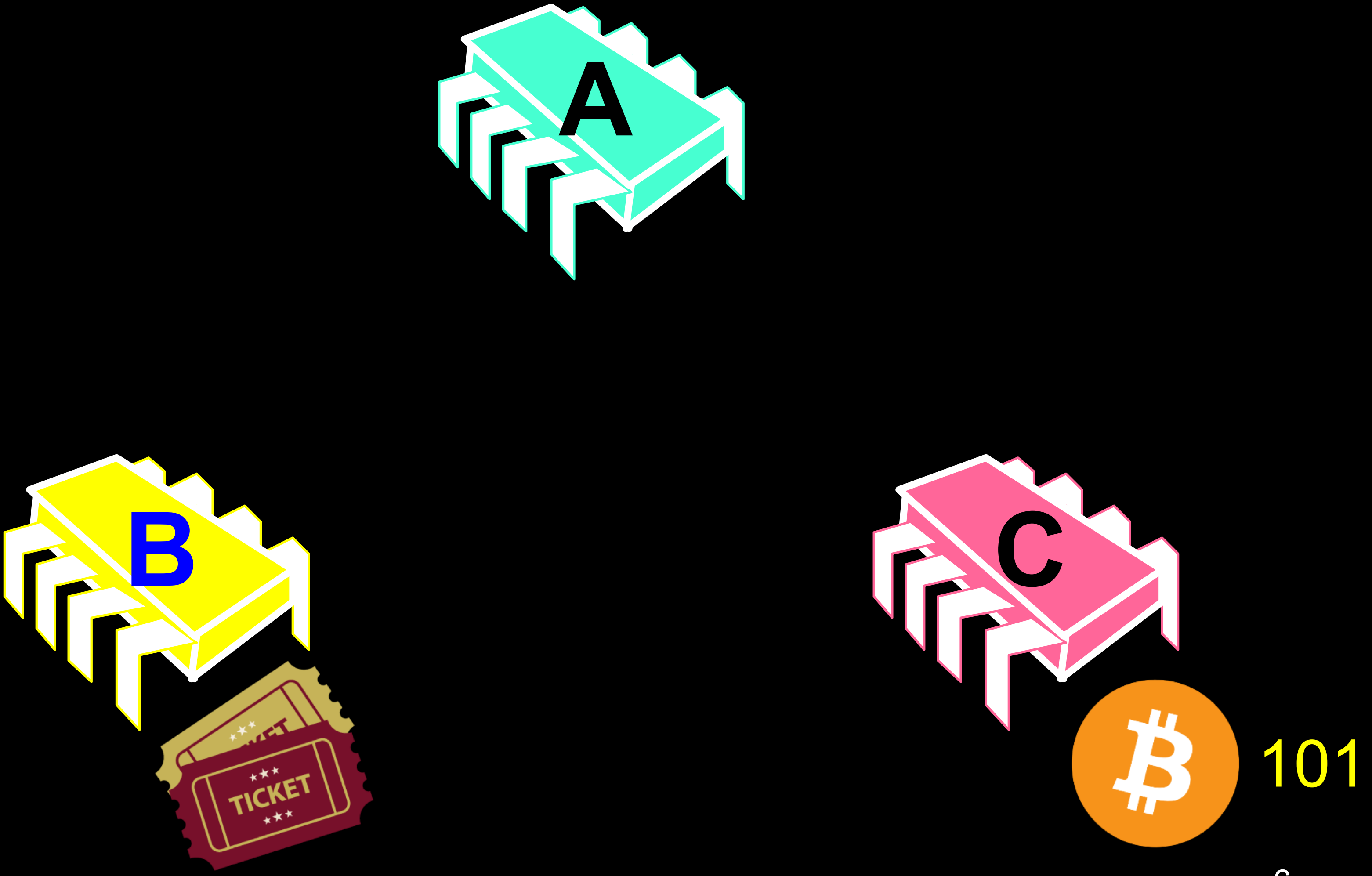


I’m Alice
I’m a ticket broker

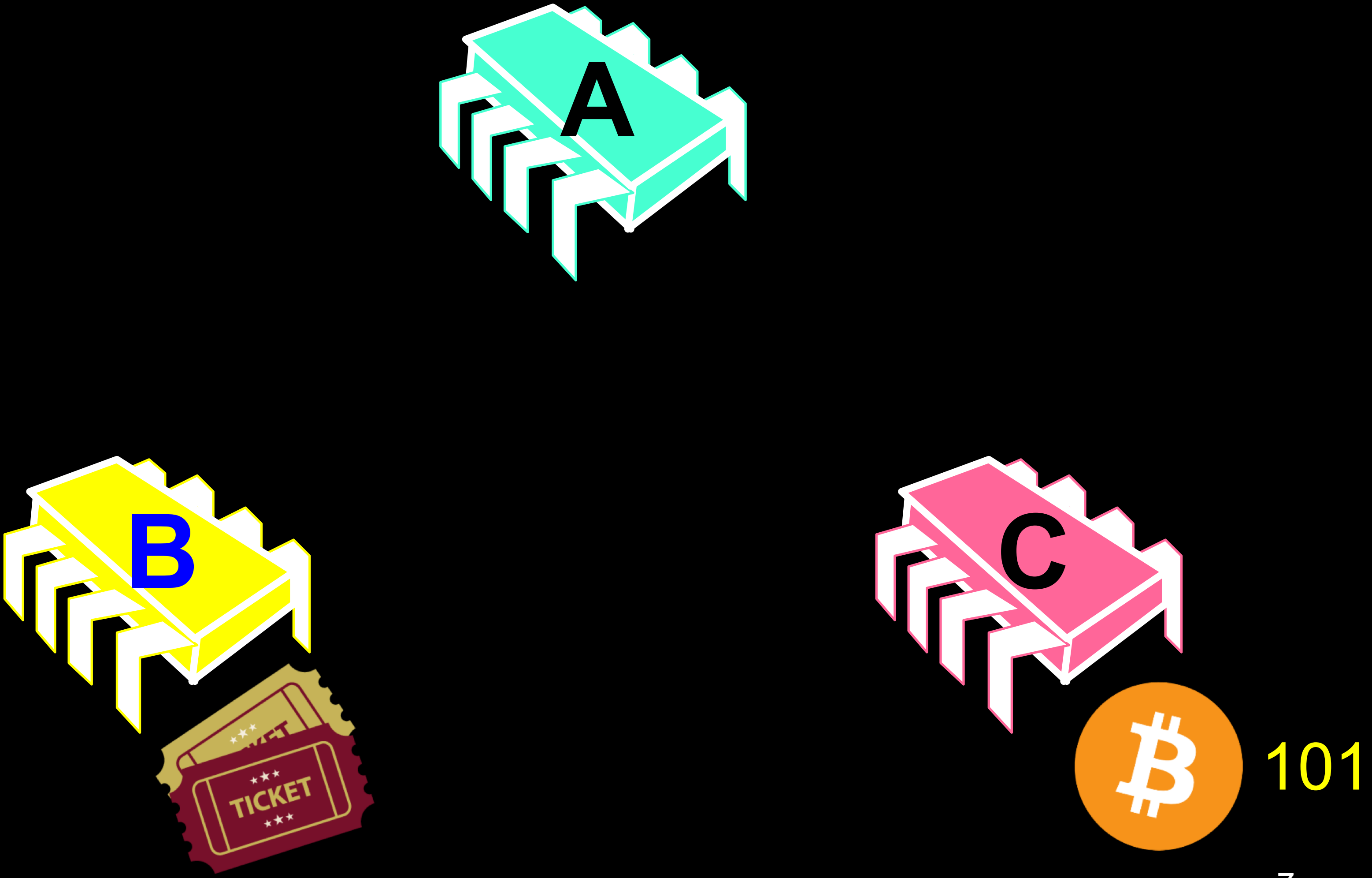
I’m Bob
I own a theater

I’m Carol
I need theater tickets

The Deal

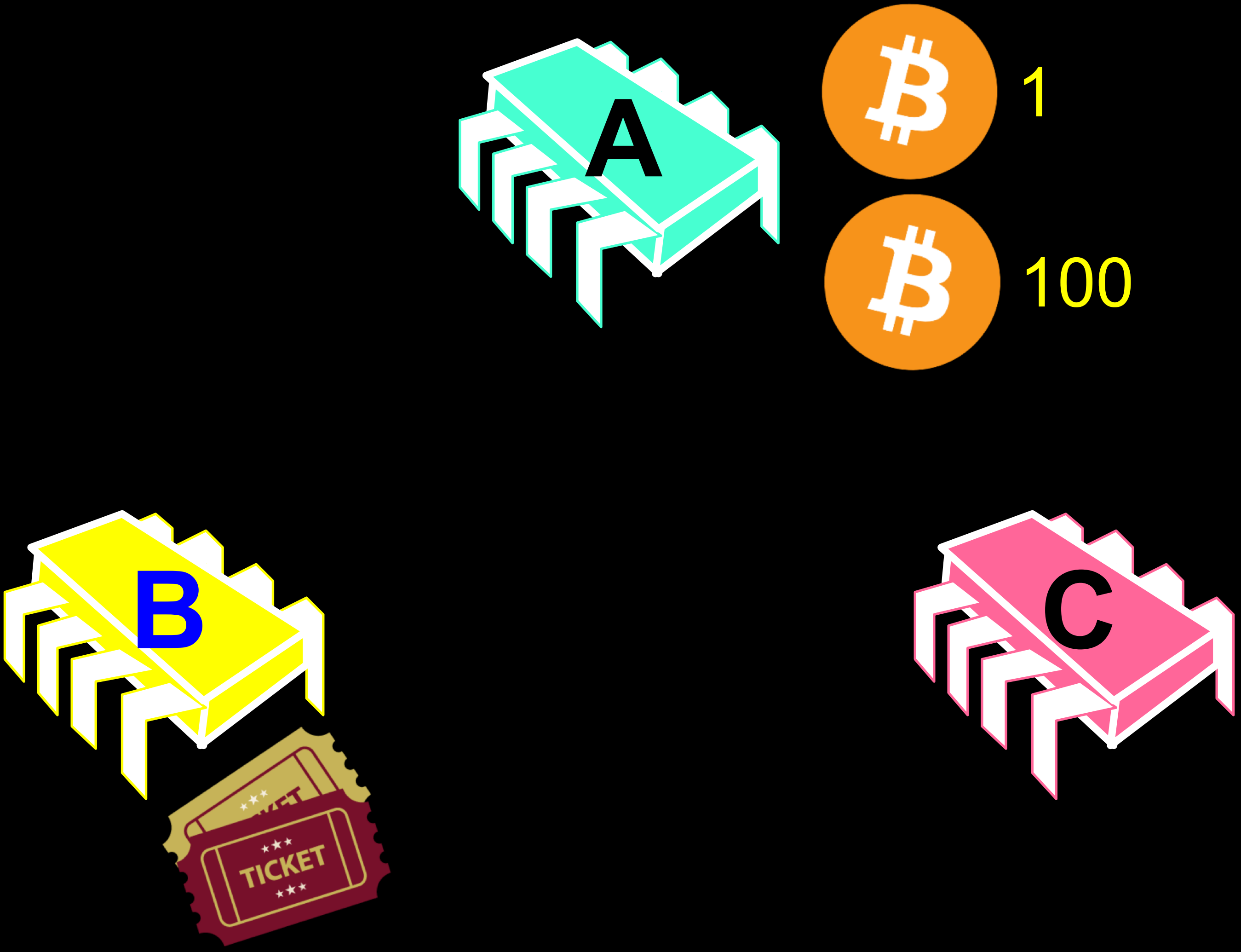


The Deal

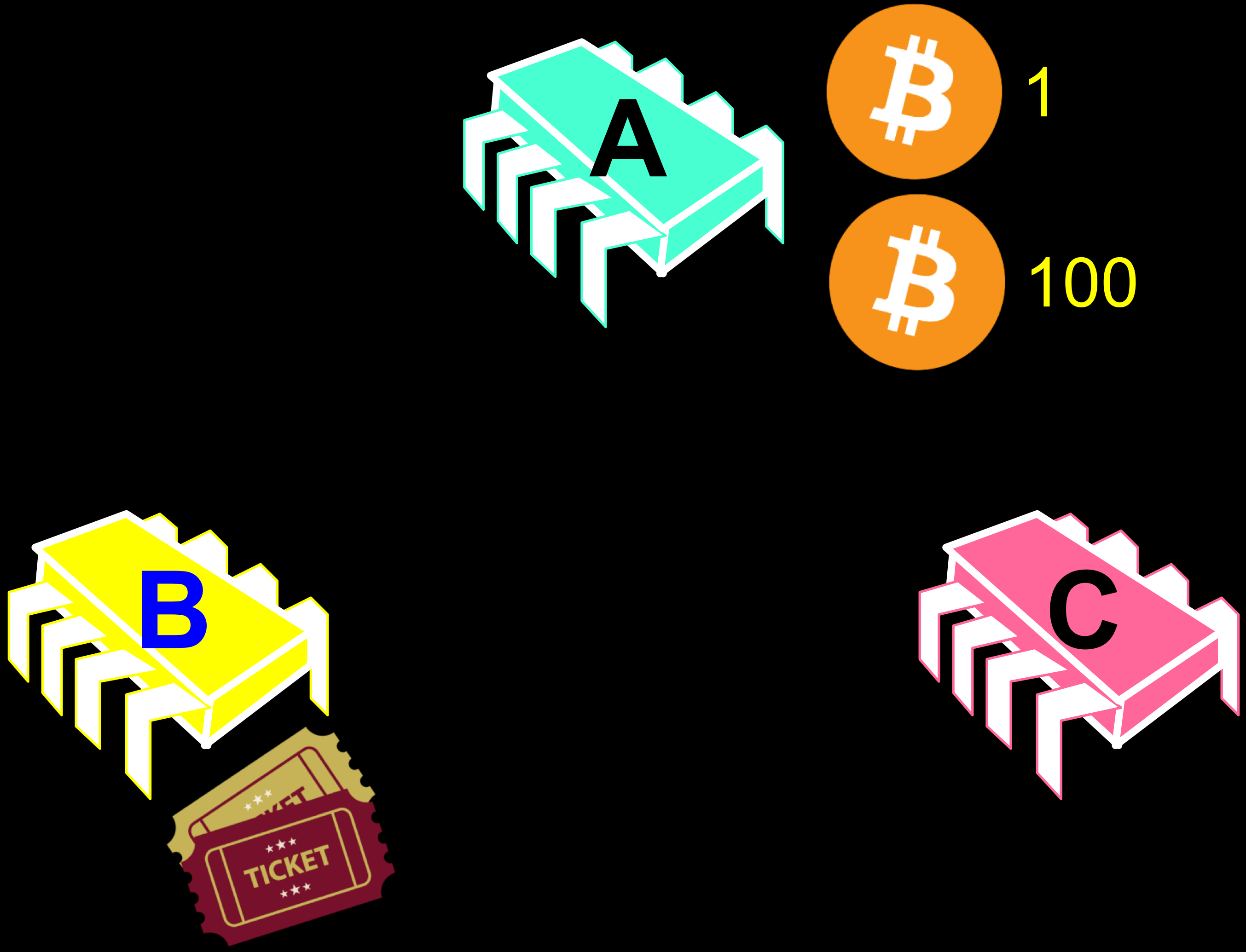


101

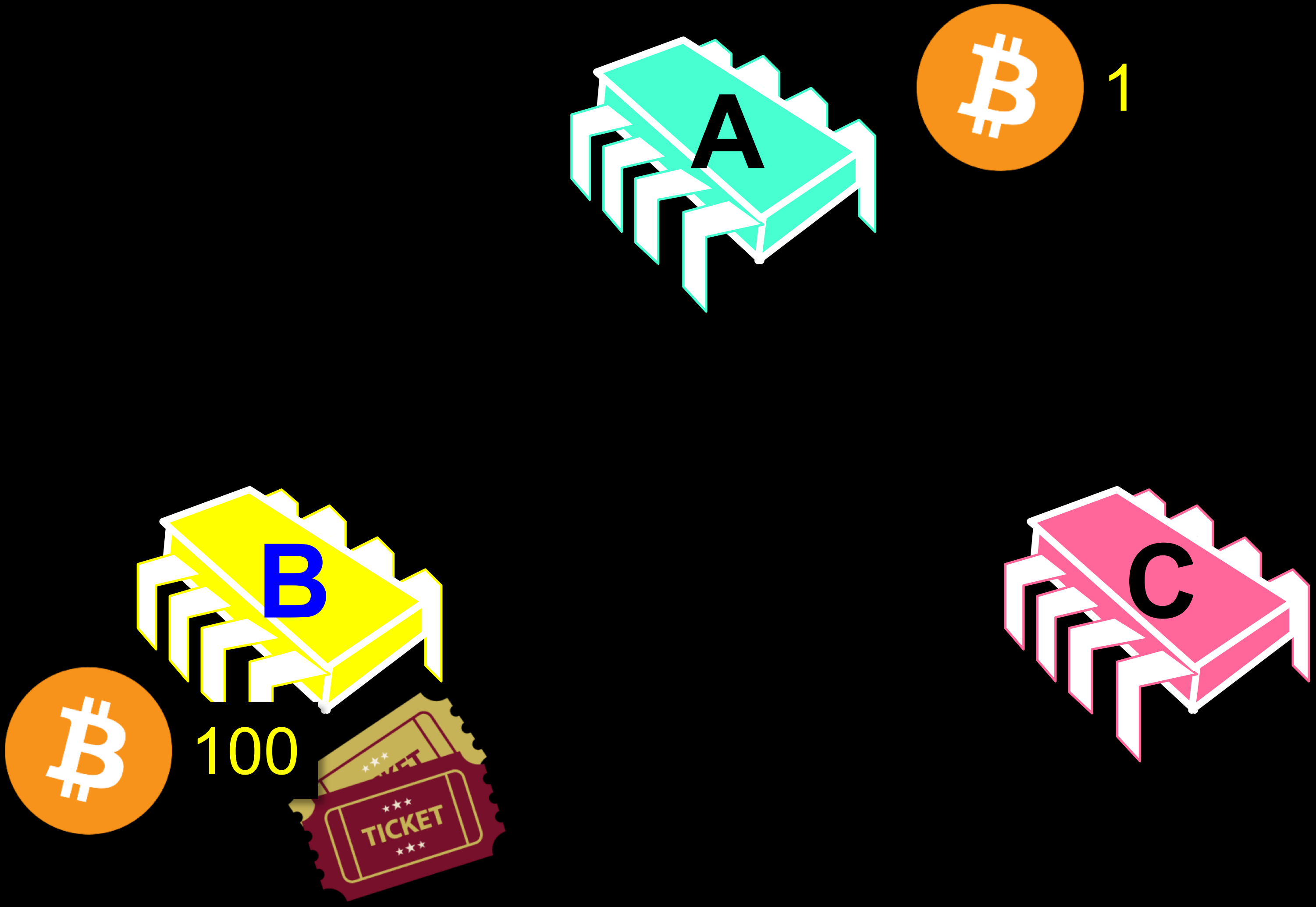
The Deal



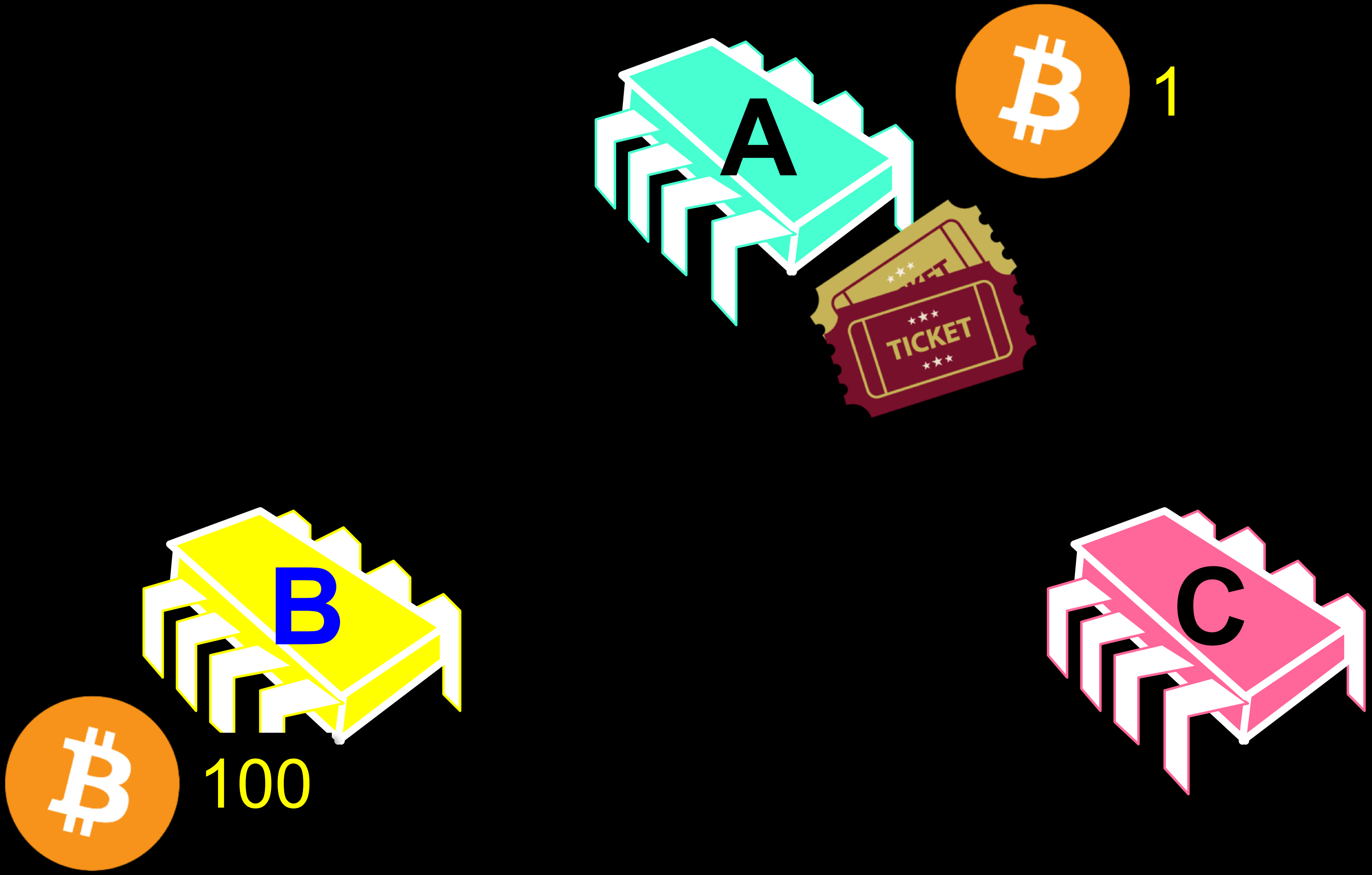
The Deal



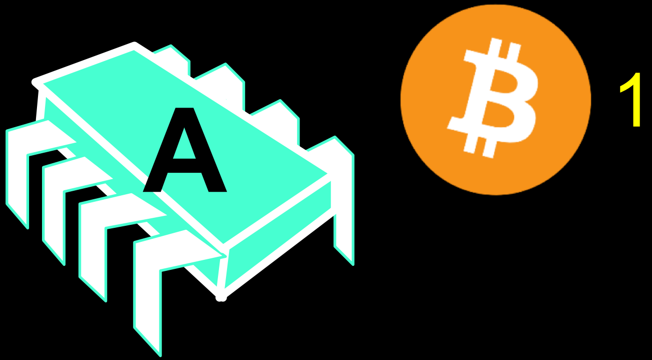
The Deal

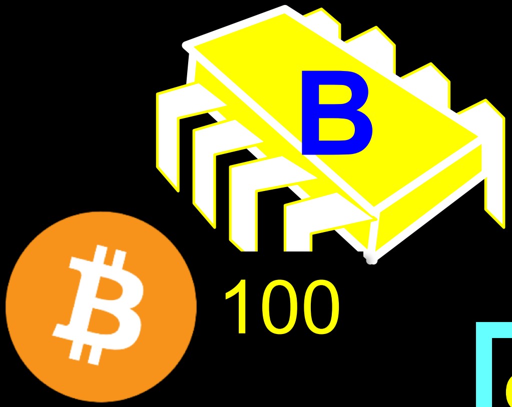


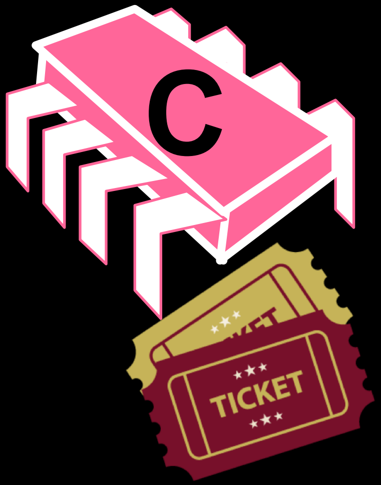
The Deal



The Deal



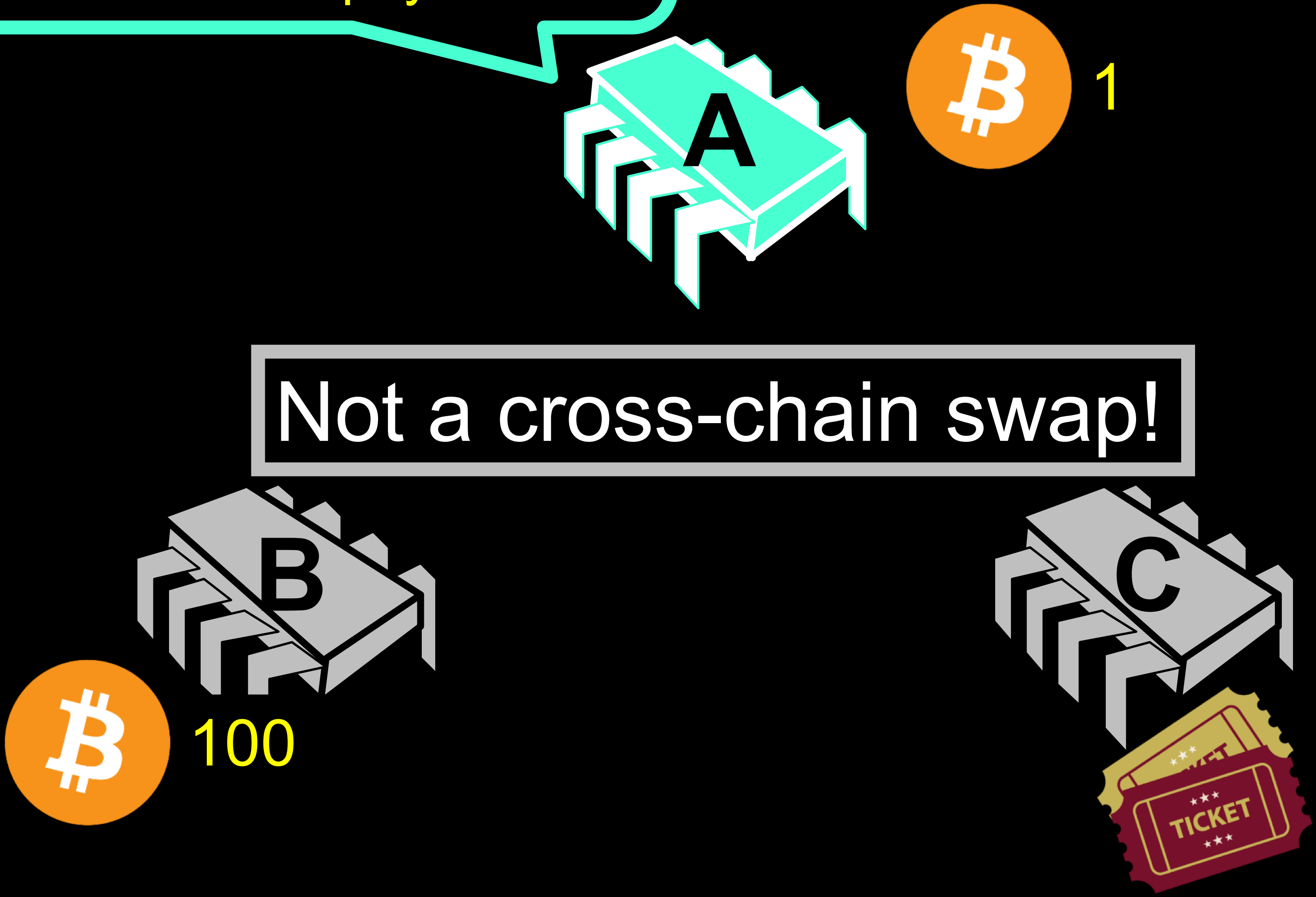




everyone happy!

Deal

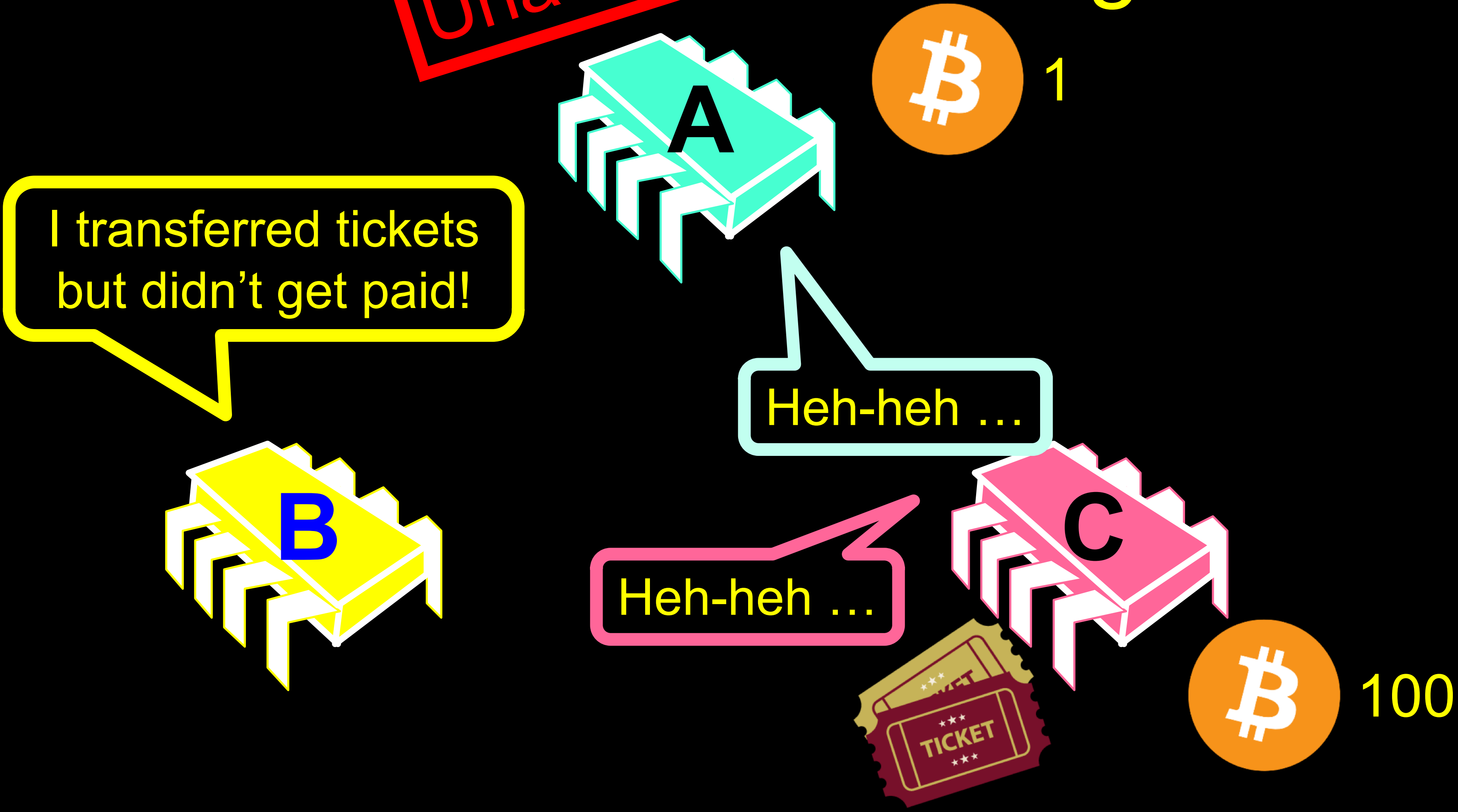
I'm using
Carol's money to pay Bob
Bob's ticket to pay Carol!



Not a cross-chain swap!

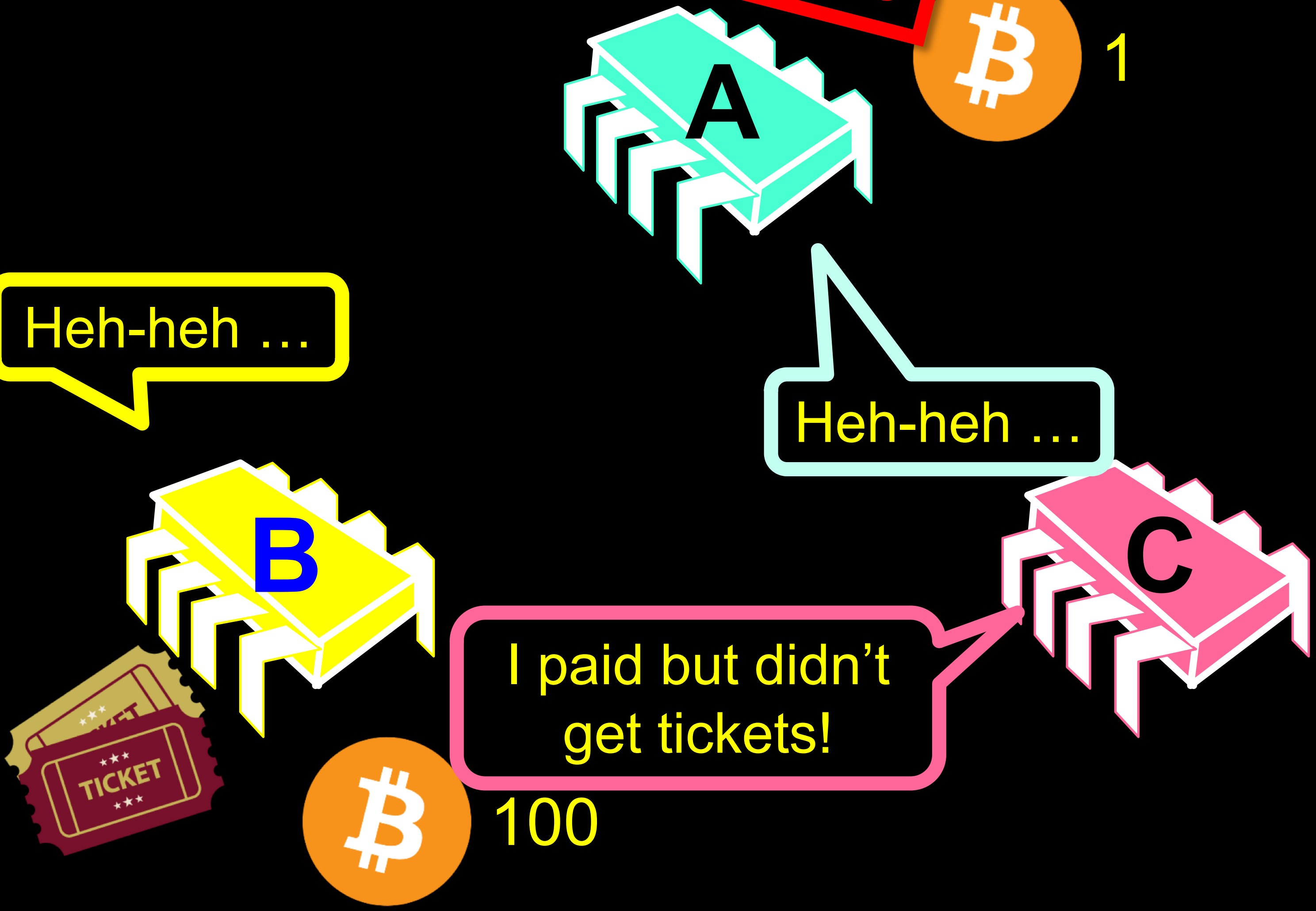
What Can Go Wrong?

Unacceptable



What Co Wrong?

Unacceptable



1

Heh-heh …

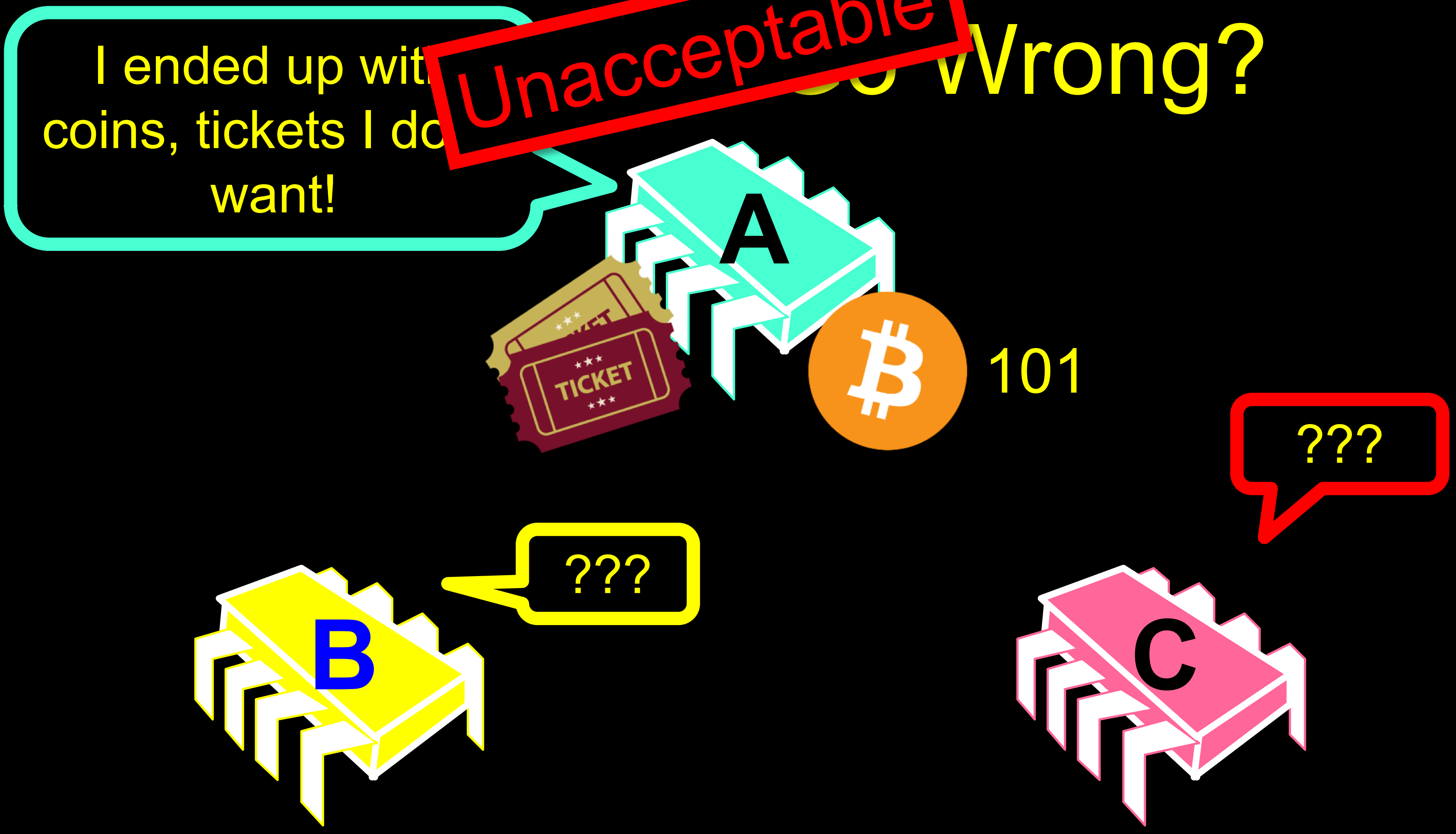
Heh-heh …

I paid but didn't get tickets!

100

Wrong?

Unacceptable



Cross-chain Deal

Bob
Felix
David
Carol
Ellen

Each party wants to trade assets …

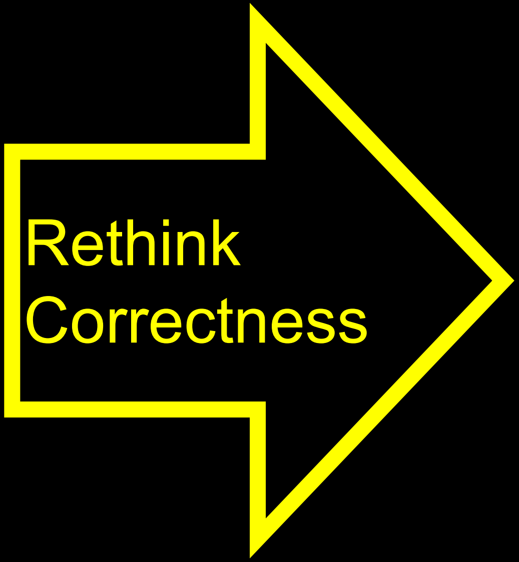
Multi-step transfers OK (not just swaps)

Each asset lives on own DB / Blockchain

No one trusts anyone

Not (exactly) a distributed transaction

This Talk



Rethink Correctness

Correctness for Classical Transactions

Atomicity

Consistency

Isolation

Durability

“ACID” properties!

Correctness for Cross-Chain Deals

Atomicity

Consistency

Isolation

Durability

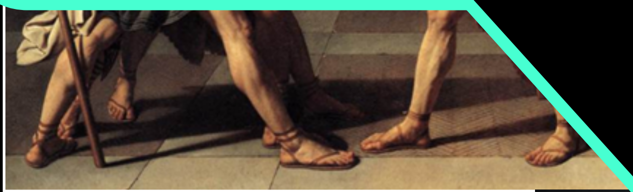
I laugh at your inadequate notions of correctness

Here is a better model

Conforming parties follow the protocol

Deviating parties might do anything

That’s it.
Not *faulty* vs *honest* vs *rational* …



Just *conforming* vs *deviating* …

Correctness for Classical Transactions

Atomicity

Either all steps happen, or none do

Isolation

Durability

All or nothing *impossible* when parties can deviate, instead …

Atomicity

Liveness: If all conform, all transfers happen

Durability

Safety: if some parties deviate, no conforming party ends up “*worse off*”

Correctness for Classical Transactions

Atomicity

Consistency

Application-specific constraints respected

Strong Nash Equilibrium

Everyone follows one strategy …

But if a coalition deviates…

It won’t improve its payoff

Correctness for Cross-Chain Deals

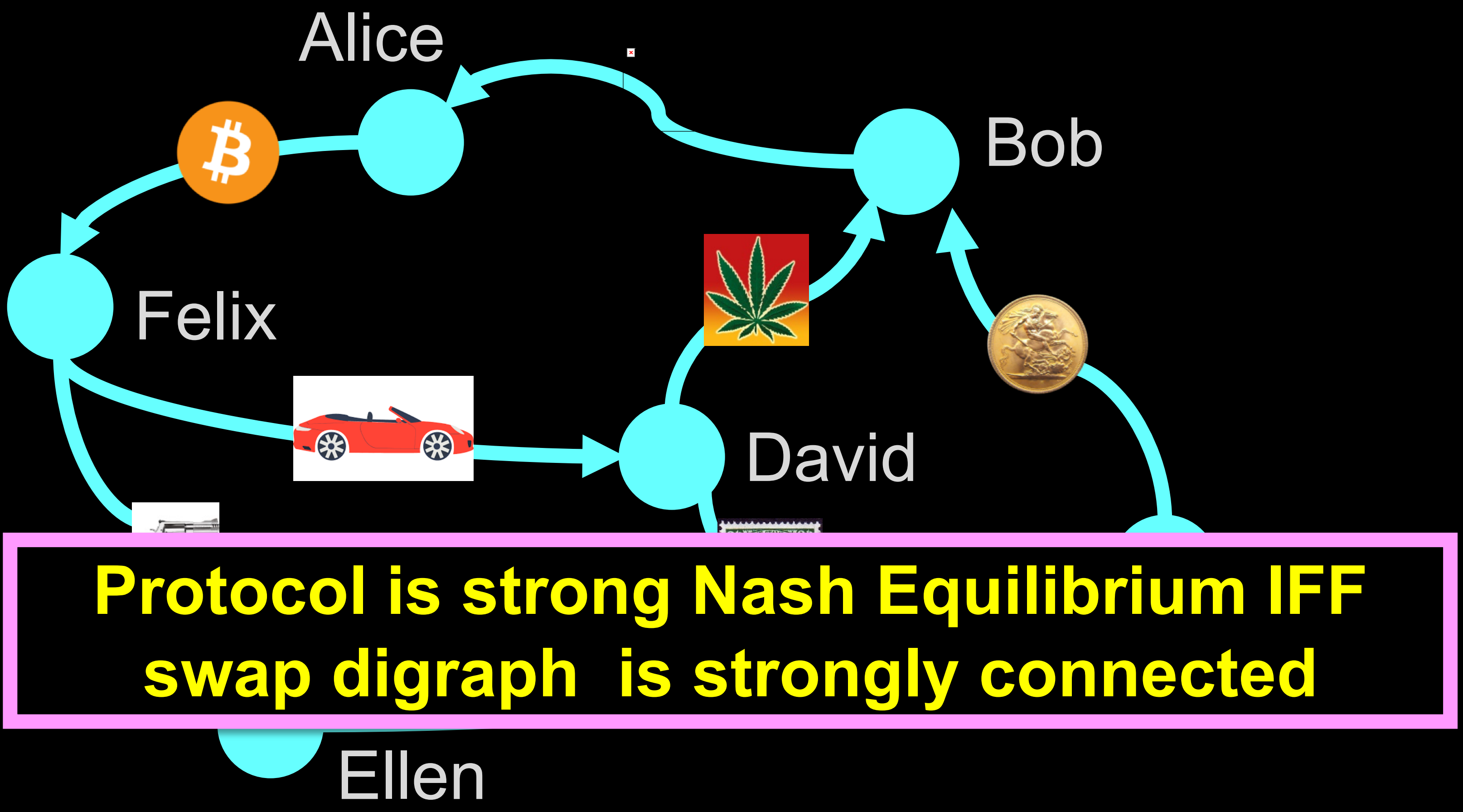
Atomicity

Consistency

Isolation

Conforming to protocol should be *strong Nash equilibrium* …

Example: Swap Digraph



Protocol is strong Nash Equilibrium IFF swap digraph is strongly connected

Correctness for Classical Transactions

No transaction sees another’s intermediate states

Consistency

Isolation

Hence serializability, snapshot consistency, etc

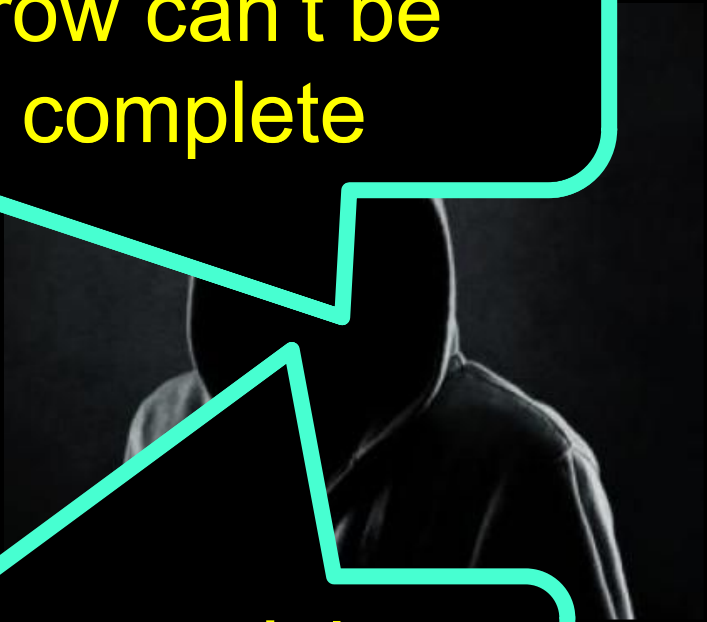
Serializability makes no sense here

Safety: “no double spending”, e.g. assets placed in escrow can’t be unlocked until deal complete

Consistency

Isolation

Durability



Liveness: But Assets can’t be escrowed forever

Correctness for Classical Transactions

Atomicity

Committed transactions survive crashes

Isolation

Durability

Correctness for
Deals

And also censorship by governments, corporations, hackers, counterparties, exes, etc

…

Durability

What We Said

Rethink Correctness

"ACID" properties for distributed transactions

Revised properties for cross-chain deals

Thank you!

Questions?

https://arxiv.org/abs/1905.09743