BITCOIN PROTOCOL AND CONSENSUS:
A HIGH LEVEL OVERVIEW

Nadir Akhtar
Gillian Chu
Brian Ho

EXPECTATIONS

Expect from us:

- A fundamental understanding of blockchain technology and its applications
- High level theory and low level technical details of bitcoin and blockchain
- Guidance and abstraction for code, CS jargon, and difficult mathematical concepts
- The best bang for your time and 2 units

We expect from you:

- Dedication -- treat this course as a 2-unit class
- Attention and readiness to learn (attendance + participation = 40% grade)
- Participation in discussion, office hours, and on Piazza to master the material
- No CS background or coding experience -- open to all majors and backgrounds

EXPECTATIONS

This class is 2 units: Attend lecture and your 1 assigned discussion

Lectures:

Saturdays 2 - 4 PM

Hearst Mining Circle 390

max. 2 lecture absences and 2 discussion absences -- more may lead to NP

Discussions:

Monday 10-11am

Tuesday 3-4pm

Wednesday 1-2pm

Wednesday 3-4pm

Thursday 12-1pm

Friday 10-11am

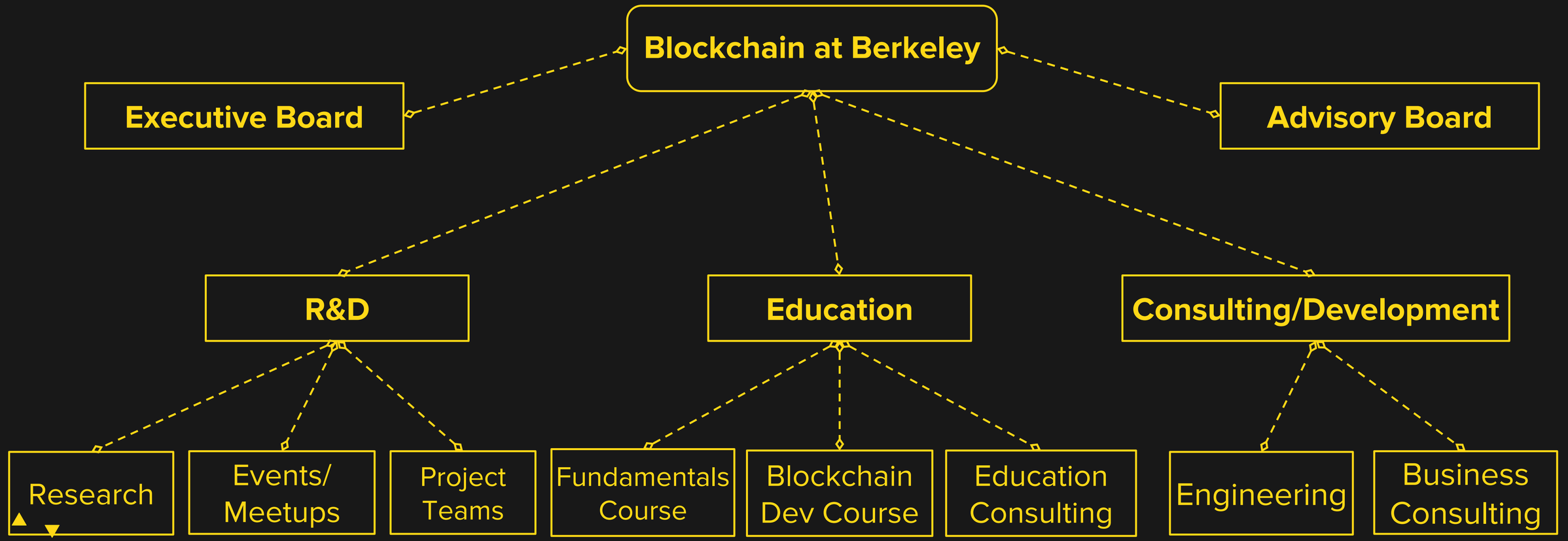
You will be assigned a discussion section later this weekend.

Enrollment codes will be handed out in discussion section THIS WEEK.

WHO ARE WE?

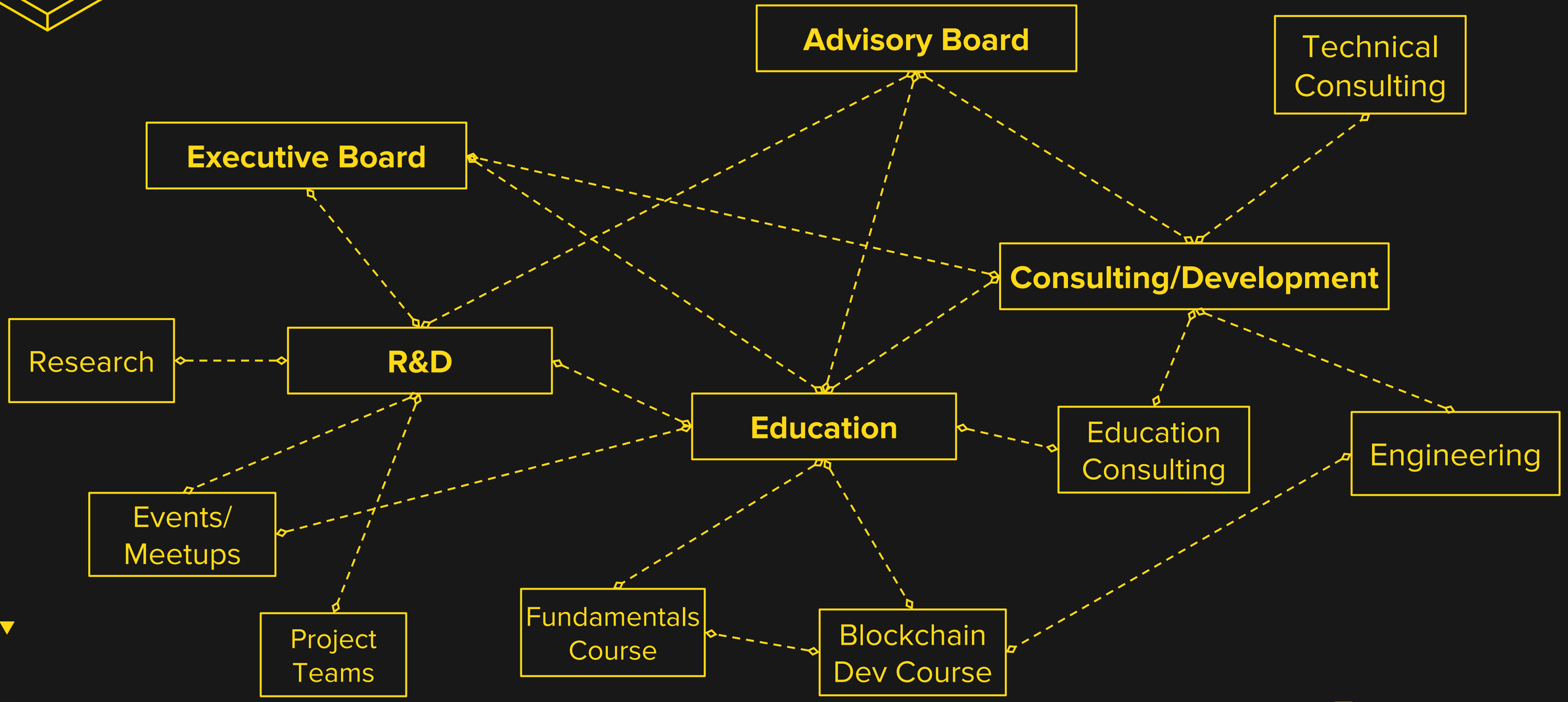
BLOCKCHAIN
AT BERKELEY

WHO ARE WE?



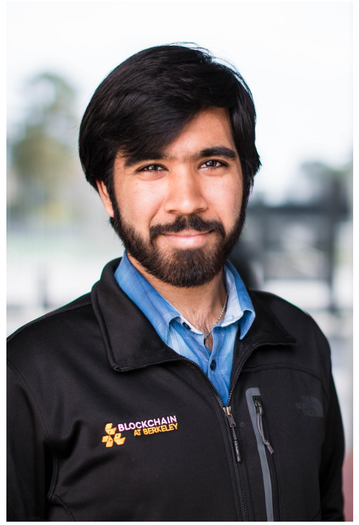
BLOCKCHAIN AT BERKELEY

WHO ARE WE?



BLOCKCHAIN AT BERKELEY

Course site: blockchain.berkeley.edu/decal/



Nadir Akhtar

nadir@blockchain.berkeley.edu

Office Hours:

- By appt

Gillian Chu

gillian@blockchain.berkeley.edu

Office Hours:

- By appt

Brian Ho

brian@blockchain.berkeley.edu

Office Hours:

- By appt

COURSE STANDARDS & RATIONALES

Standards:

- 1 HW, one quiz a week (unless otherwise noted) + readings
- Black slides for **technical material**
- Openness to questions, no matter how “stupid” (but may defer off topic questions to discussion)
- Two epochs:
  1. Cryptocurrencies: Bitcoin and the Crypto Space
  2. Blockchain: Advancing Decentralized Tech

Rationales:

- Build up the highest possible mental model before delving into specifics
  - Build an image with the “lowest-resolution” puzzle pieces before breaking down each piece
- Lectures for learning, discussions for discussing
  - Your spot is *very* valuable -- one and a half people cannot be here today because you were deemed worthy

QUESTIONS?

BITCOIN PROTOCOL AND CONSENSUS:
A HIGH LEVEL OVERVIEW

Nadir Akhtar
Gillian Chu
Brian Ho

BLOCKCHAIN
AT BERKELEY

LECTURE OVERVIEW

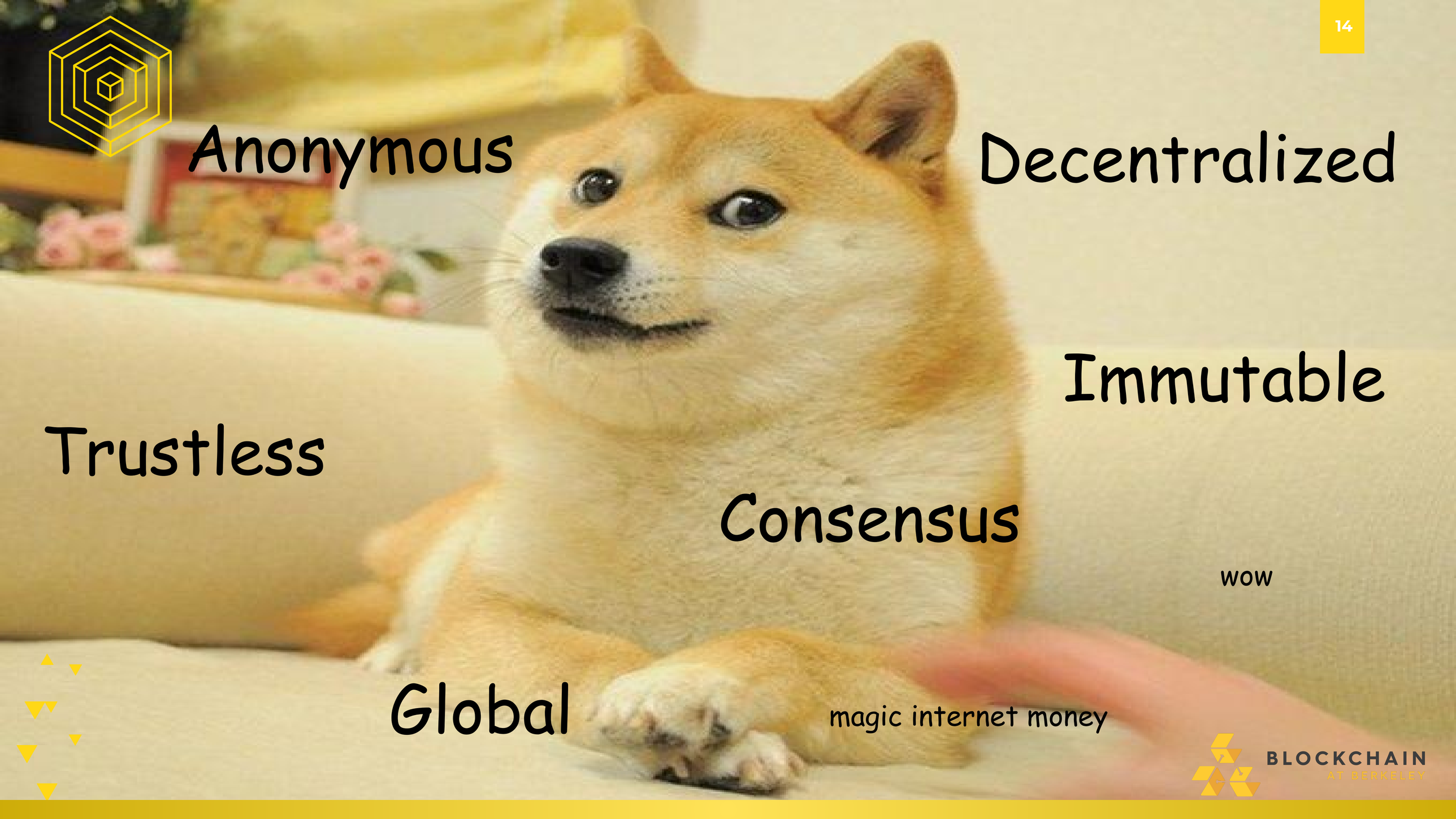
1. WHAT IS BITCOIN?
2. IDENTITY
3. TRANSACTIONS
4. RECORD-KEEPING (THE BLOCKCHAIN)
5. CONSENSUS (PROOF-OF-WORK)

1 WHAT IS BITCOIN?

WHAT IS BITCOIN?

BITCOIN'S GENESIS

- Bitcoin is a cryptocurrency, existing purely in the digital realm, first deployed in 2009.
  - **Cryptocurrency:** a currency built upon computer science, cryptography, and economics
- Born out of the Cypherpunk movement, a libertarian fight for privacy and self-governance.
- The inspiration for the invention of the blockchain.
- Created by Satoshi Nakamoto, an anonymous identity.


Anonymous
Decentralized
Immutable
Trustless
Consensus
wow
Global
magic internet money

CURRENCY

“IN BANKS WE DISTRUST”

What does a bank provide?

- Account and identity management: Storage of your personal information and your account balances
- Services: Transferring and redeeming money
- Record management: Tracking account history, particularly for audits
- Trust: Verified professionals regulated by gov’t

How do we make a decentralized system that does everything that a bank does?

CURRENCY

“IN BITCOIN WE TRUST”

What does Bitcoin provide?

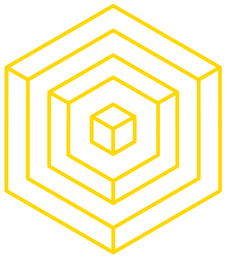
- Account and identity management: Addresses for every user, each associated with amounts of currency
- Services: Transactions between users done by *other users*
- Record management: Redundant information stored between thousands of users via a **blockchain**
- Trust: Personal incentive aligning with community goals

But how does this all happen?

Image source:
https://s3.amazonaws.com/kd4/byob

QUESTIONS?

2 IDENTITY



IDENTITY

IDENTITY IN BITCOIN

"What's the role of identity in the context of currencies?"

IDENTITY

IDENTITY IN BITCOIN

- What's the role of identity in the context of currencies?
  - **Receiving** money
  - **Claiming/Spending** money
  - **Blame**
- Identity in daily life:
  - Houses have addresses and mailbox keys
  - Emails have aliases and passwords
  - Bitcoin has public keys and private keys

IDENTITY

PUBLIC AND PRIVATE KEYS

- Each entity is represented with a unique **public key**
  - A corresponding **private key** acts as a key to “unlock” the public key, the proverbial chest containing your money
- Private key chosen at random, public key generated from private key
  - **Public key** for *receiving*, **private key** for *redeeming*
- Note: address =/= public key in reality -- we’ll make the distinction clear in Lecture 3

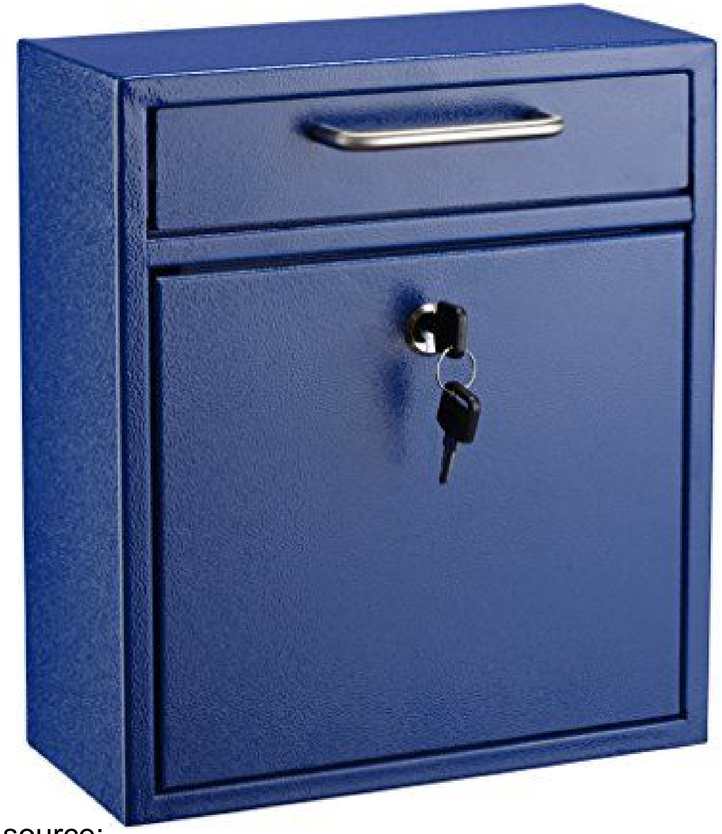


Image source: https://images-na.ssl-images-amazon.com/images/I/51rh0s9VdyL.jpg

IDENTITY

PUBLIC KEY SECURITY

https://www.shutterstock.com/image-illustration/sandy-planet-earth-sand-gravel-pebbles-66233314

IDENTITY

PUBLIC KEY SECURITY

https://www.shutterstock.com/image-illustration/sandy-planet-earth-sand-gravel-pebbles-66233314

IDENTITY

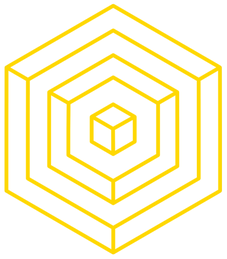
SECURITY: HIDDEN IN PLAIN SIGHT

“What if someone guesses my private key?!”

- Bitcoin is hidden in the large amount of public keys
  - 2^{160} (1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,97) possible addresses
- Practically impossible for anyone to overlap using random generation of public key
  - For reference:
    - Grains of sand on earth: 2^{63}
    - With 2^{63} earths, each with 2^{63} grains of sand: 2^{126} total grains of sand
    - 2^{126} is only **0.0000000058%** of 2^{160}
  - Population of world: 7.5 billion in April 2017
    - Every person could have about 2^{127} addresses *all to themselves*

QUESTIONS?

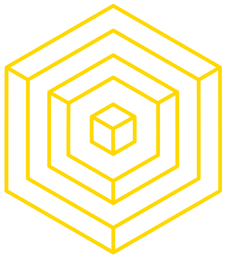
3 TRANSACTIONS



TRANSACTIONS

VALIDITY

"What makes a transaction valid?"



TRANSACTIONS

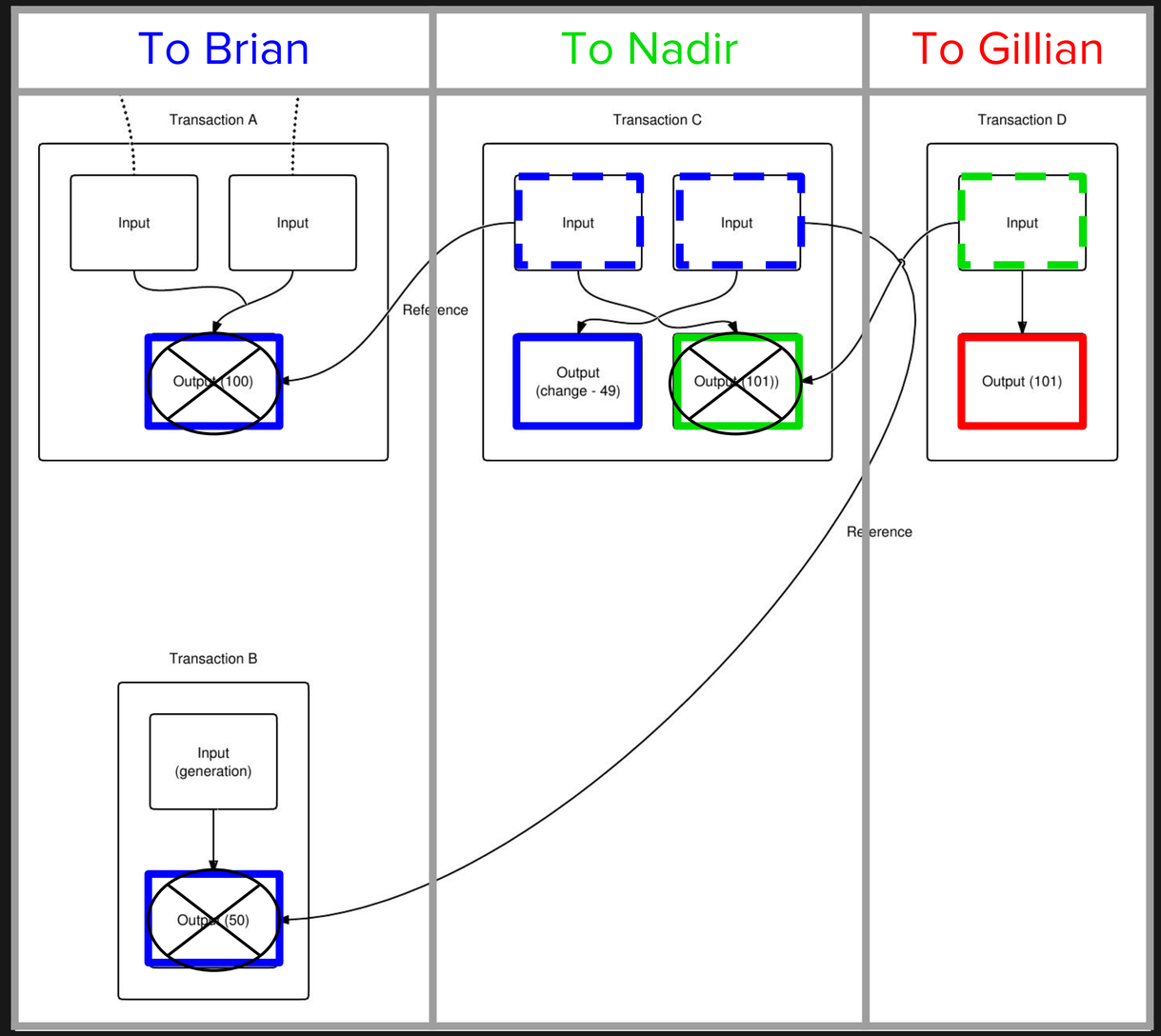
VALIDITY

- What makes a transaction valid?
  - Proof of ownership (a signature)
  - Available funds
  - No other transactions using the same funds

TRANSACTIONS

UTXO MODEL

- **Unspent Transaction Output (UTXO)**
  - Bitcoin’s model for transactions
- **Chests** (accounts) vs **Piggy banks** (UTXOs)



Source: https://en.bitcoin.it/wiki/File:Transaction.png

QUESTIONS?

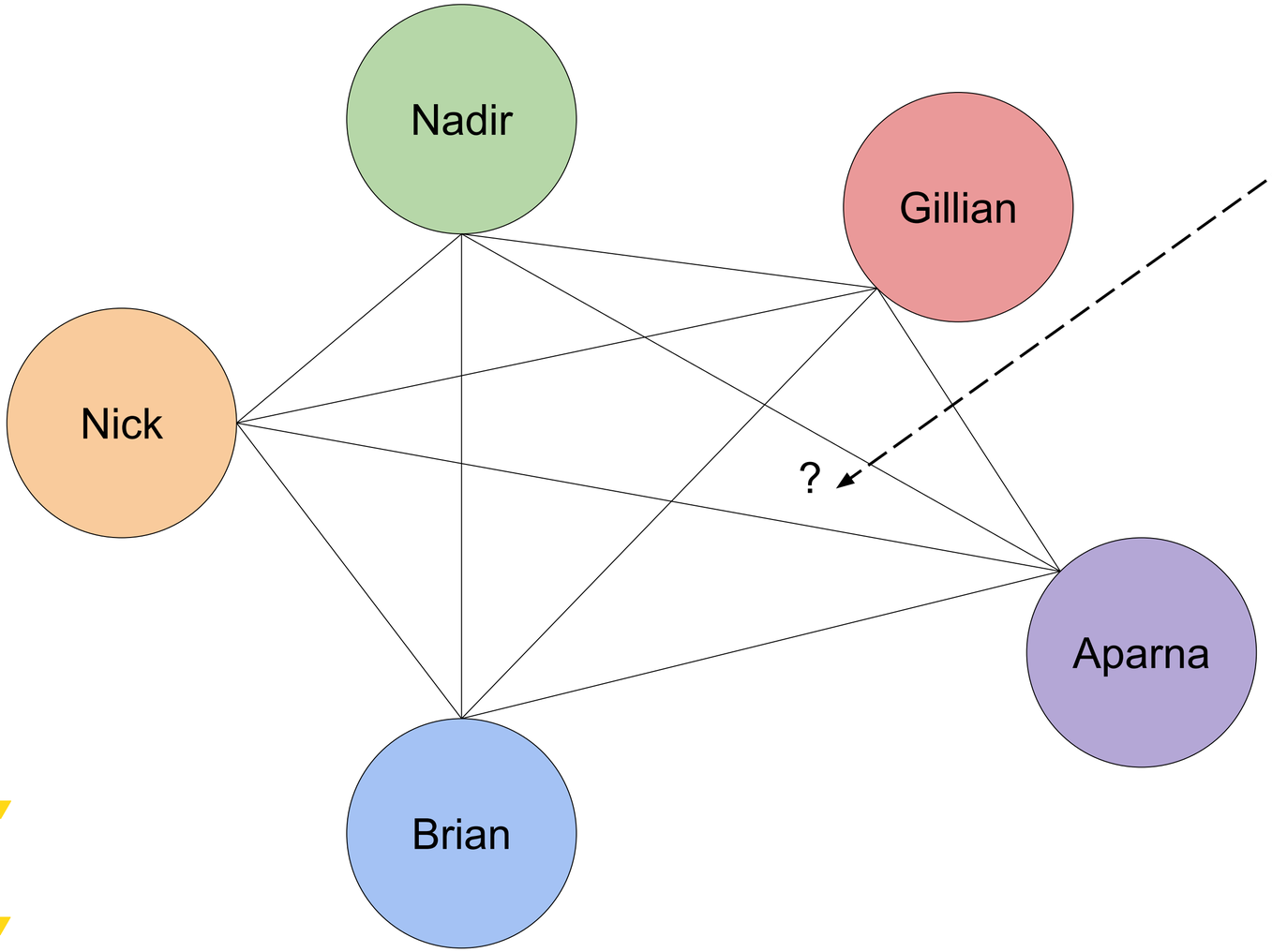
BREAK SECTION

BLOCKCHAIN AT BERKELEY

4 RECORD-KEEPING: THE BLOCKCHAIN

RECORD-KEEPING

DISTRIBUTED DATABASES



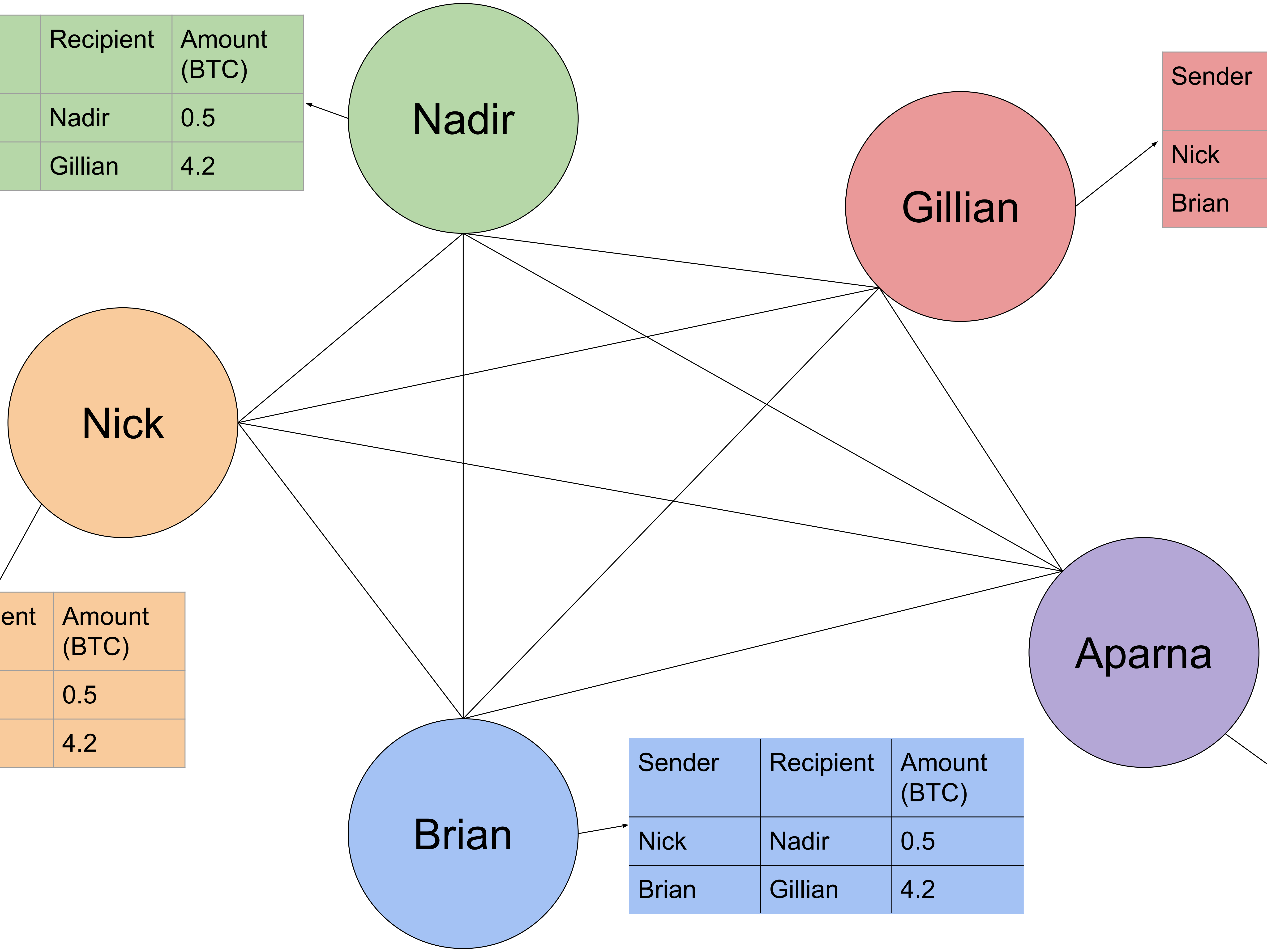
Sender	Recipient	Amount (BTC)
Nick	Nadir	0.5
Brian	Gillian	4.2

We know how to represent identities and transactions---how do we store all that information? How do we keep track of this ledger of transactions?

⇒ With a **distributed database**

RECORD-KEEPING

EVERYONE'S THE BANK



Sender	Recipient	Amount (BTC)
Nick	Nadir	0.5
Brian	Gillian	4.2

Sender	Recipient	Amount (BTC)
Nick	Nadir	0.5
Brian	Gillian	4.2

Everyone stores the ledger

Sender	Recipient	Amount (BTC)
Nick	Nadir	0.5
Brian	Gillian	4.2

Sender	Recipient	Amount (BTC)
Nick	Nadir	0.5
Brian	Gillian	4.2

Sender	Recipient	Amount (BTC)
Nick	Nadir	0.5
Brian	Gillian	4.2

RECORD-KEEPING

THE BLOCKCHAIN

Sender	Recipient	Amount (BTC)
Nick	Nadir	0.5
Brian	Gillian	4.2
Aparna	Gillian	23
Nick	Aparna	3.2
Nadir	Brian	0.3
Gillian	Aparna	17

Batching

Sender	Recipient	Amount (BTC)
Nick	Nadir	0.5
Brian	Gillian	4.2

Sender	Recipient	Amount (BTC)
Aparna	Gillian	23
Nick	Aparna	3.2

Sender	Recipient	Amount (BTC)
Nadir	Brian	0.3
Gillian	Aparna	17

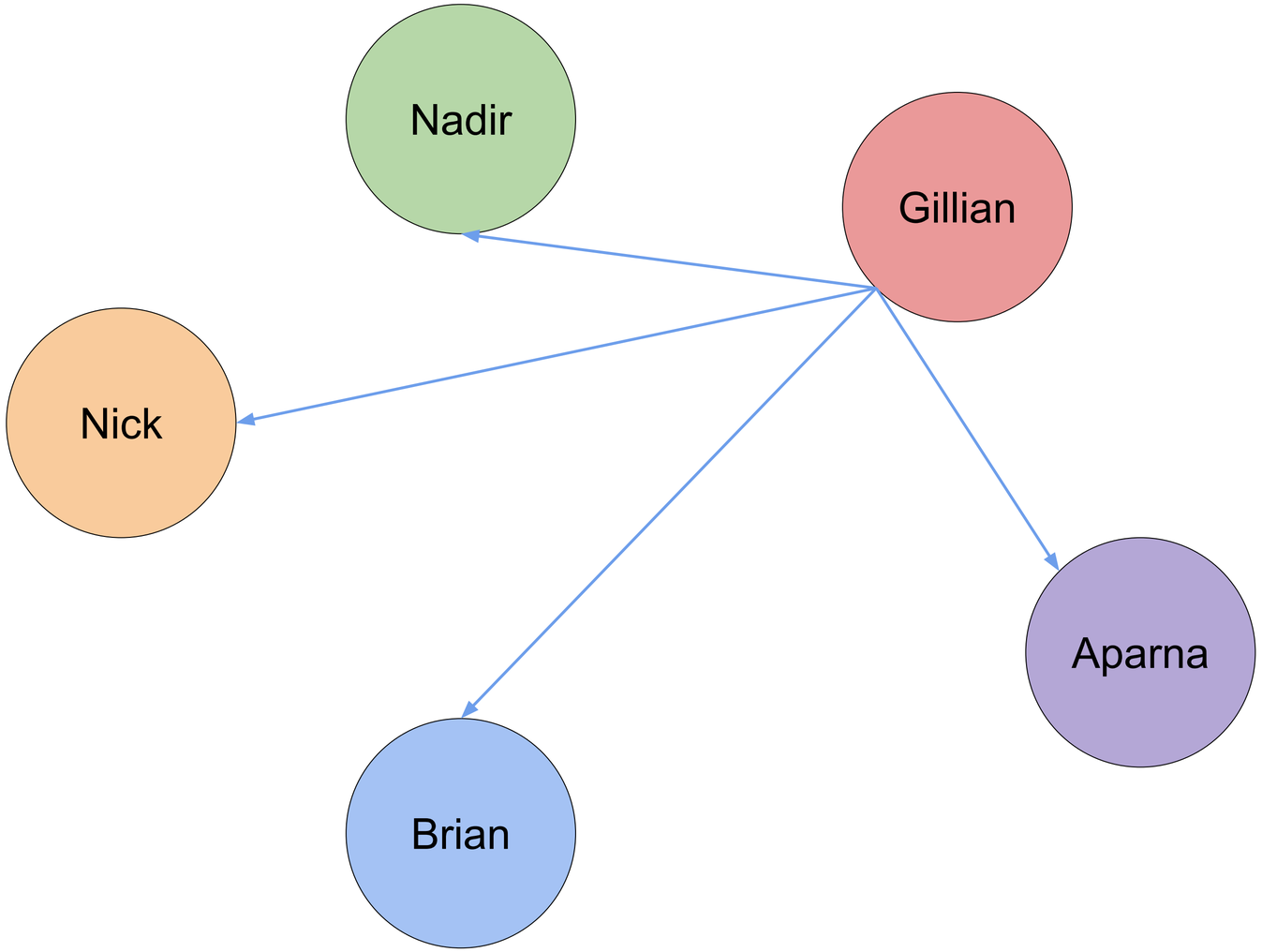
QUESTIONS?

5

CONSENSUS (PROOF-OF-WORK)

CONSENSUS

STAYING ON THE SAME PAGE

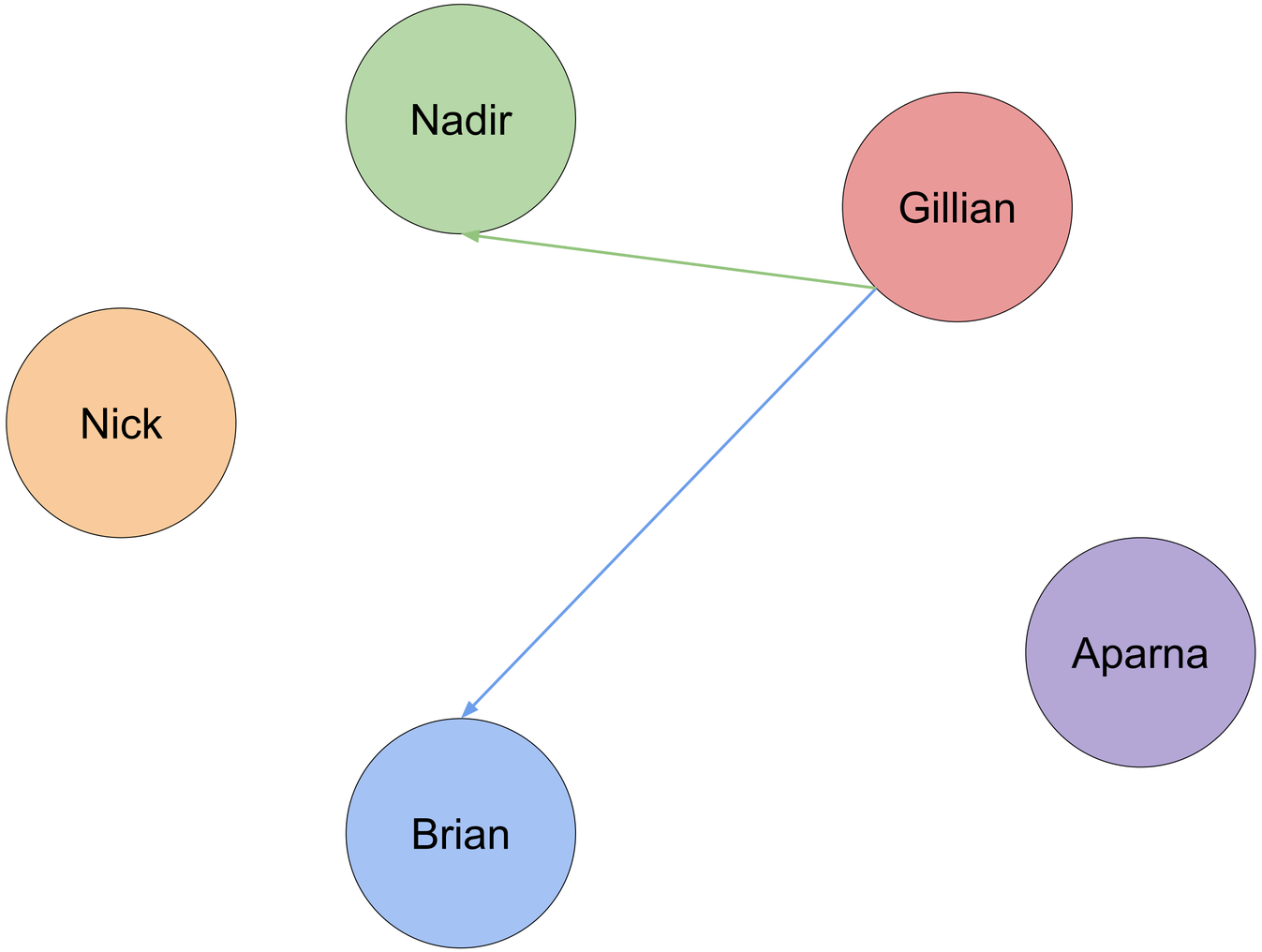


Everyone accepts valid transactions as they come around without “discussion”

- How do we ensure no one’s cheating if we make decisions alone?

CONSENSUS

DOUBLE SPEND ATTACK

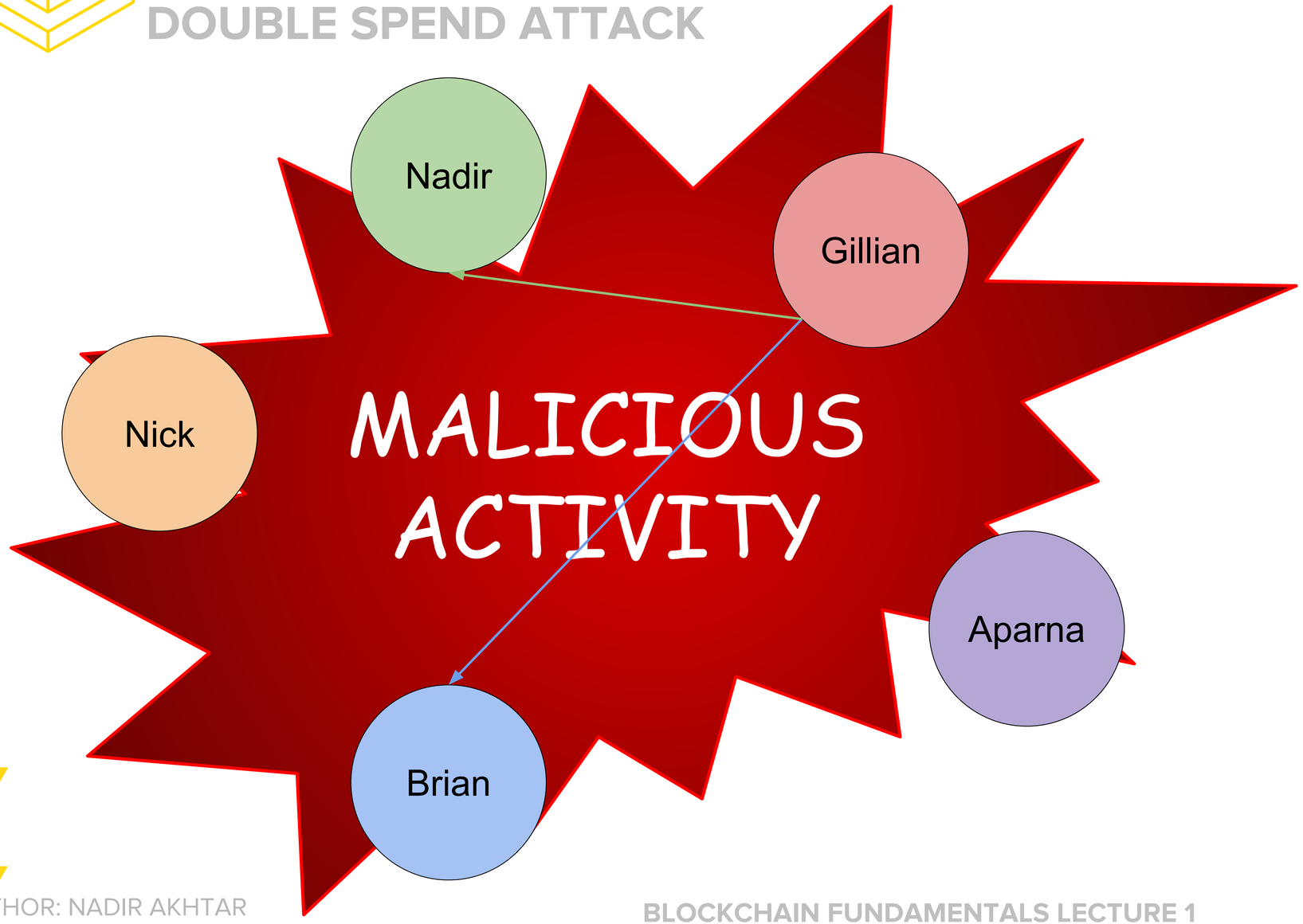


Gillian promises 10 BTC to Brian in one transaction, and she promises 10 BTC to Nadir in another -- but she only has 10 BTC total!

- Gillian is performing a **double spend** attack

CONSENSUS

DOUBLE SPEND ATTACK

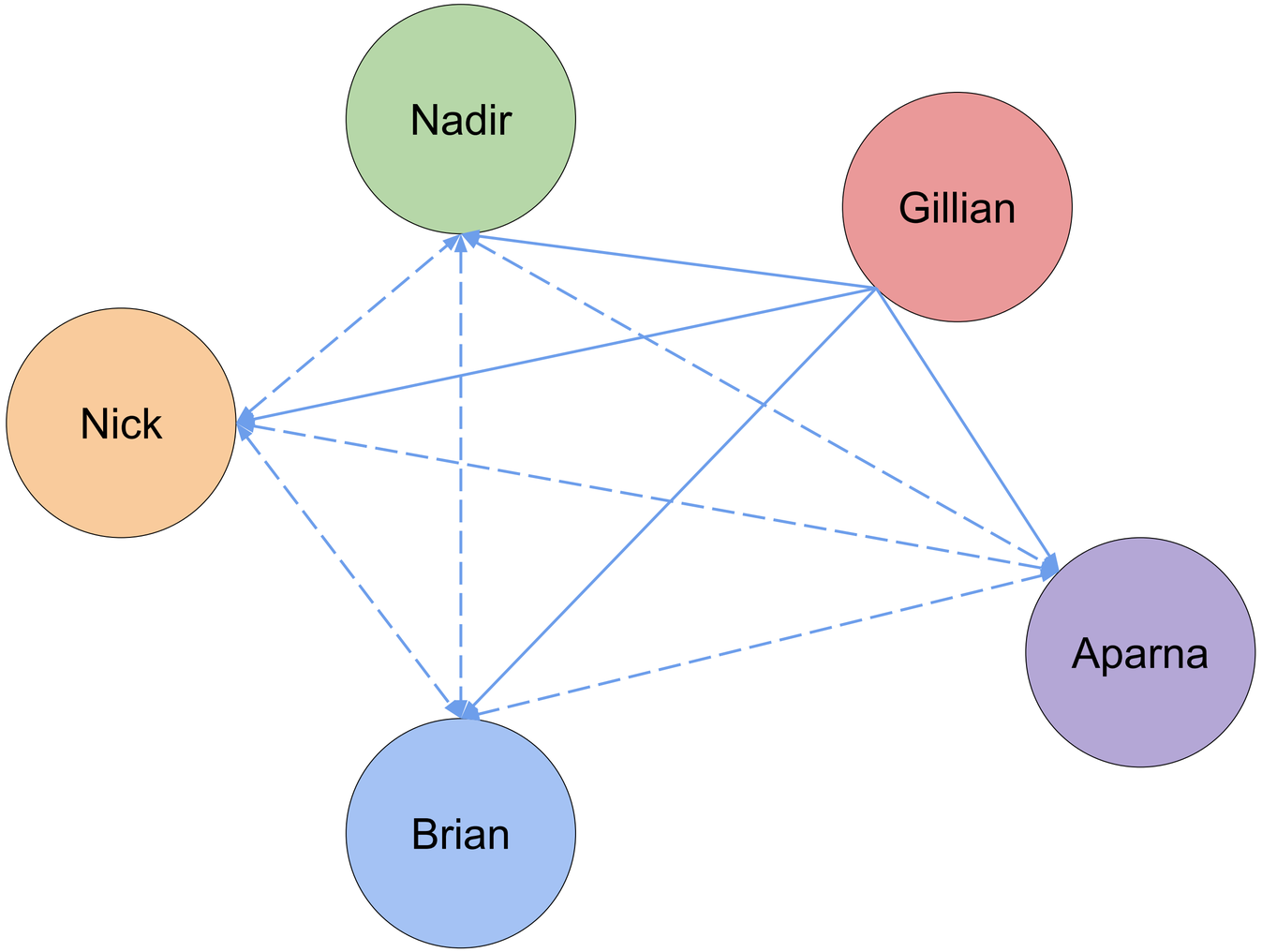


Gillian promises 10 BTC to Brian in one transaction, and she promises 10 BTC to Nadir in another -- but she only has 10 BTC total!

- Gillian is performing a **double spend** attack

CONSENSUS

PEER VALIDATION

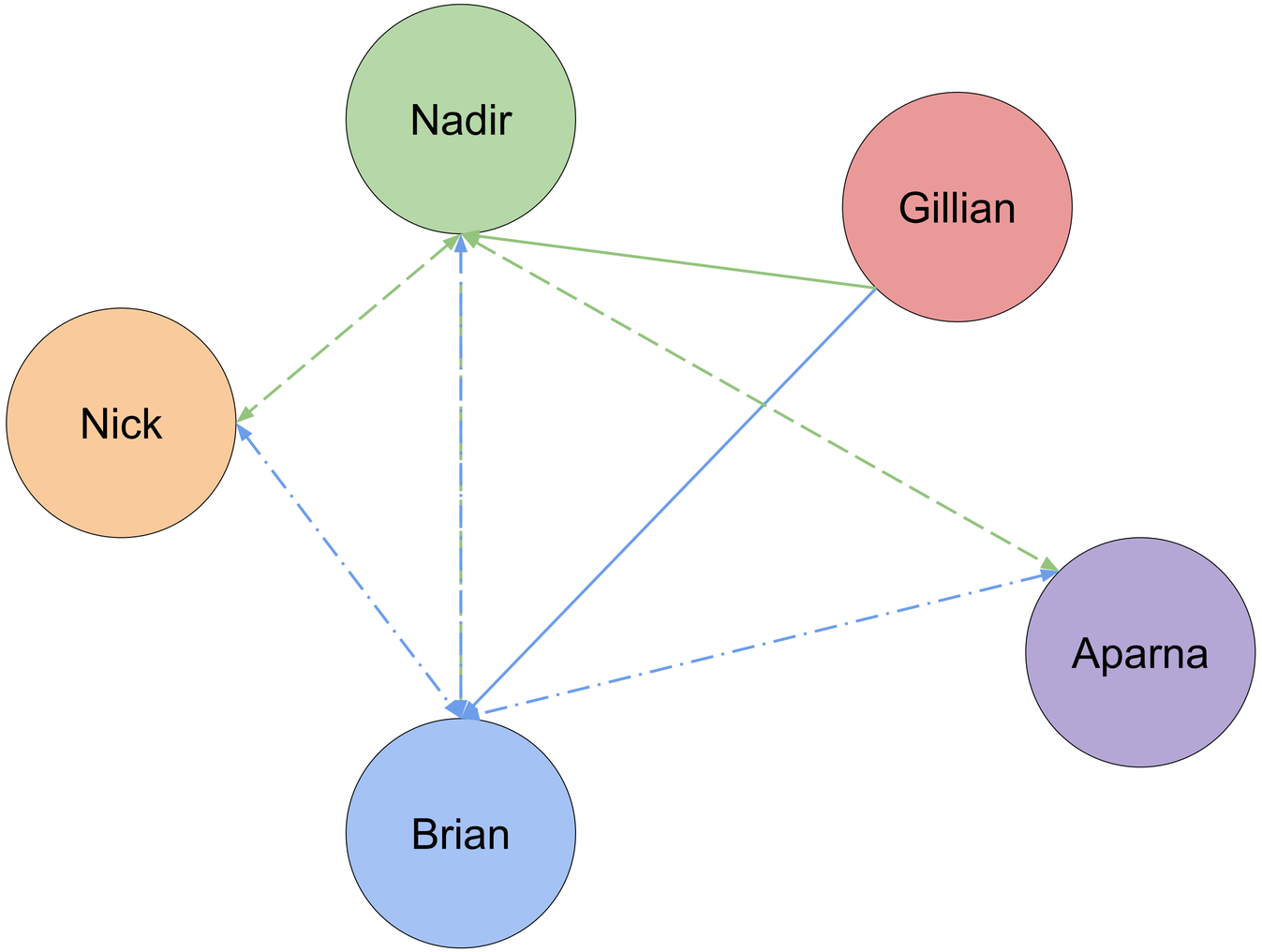


Instead of siloed decisions, let's have proposers and voters

- The proposer submits a transaction to everyone else
- Peers cast votes
- Only save after receiving a certain number of votes

CONSENSUS

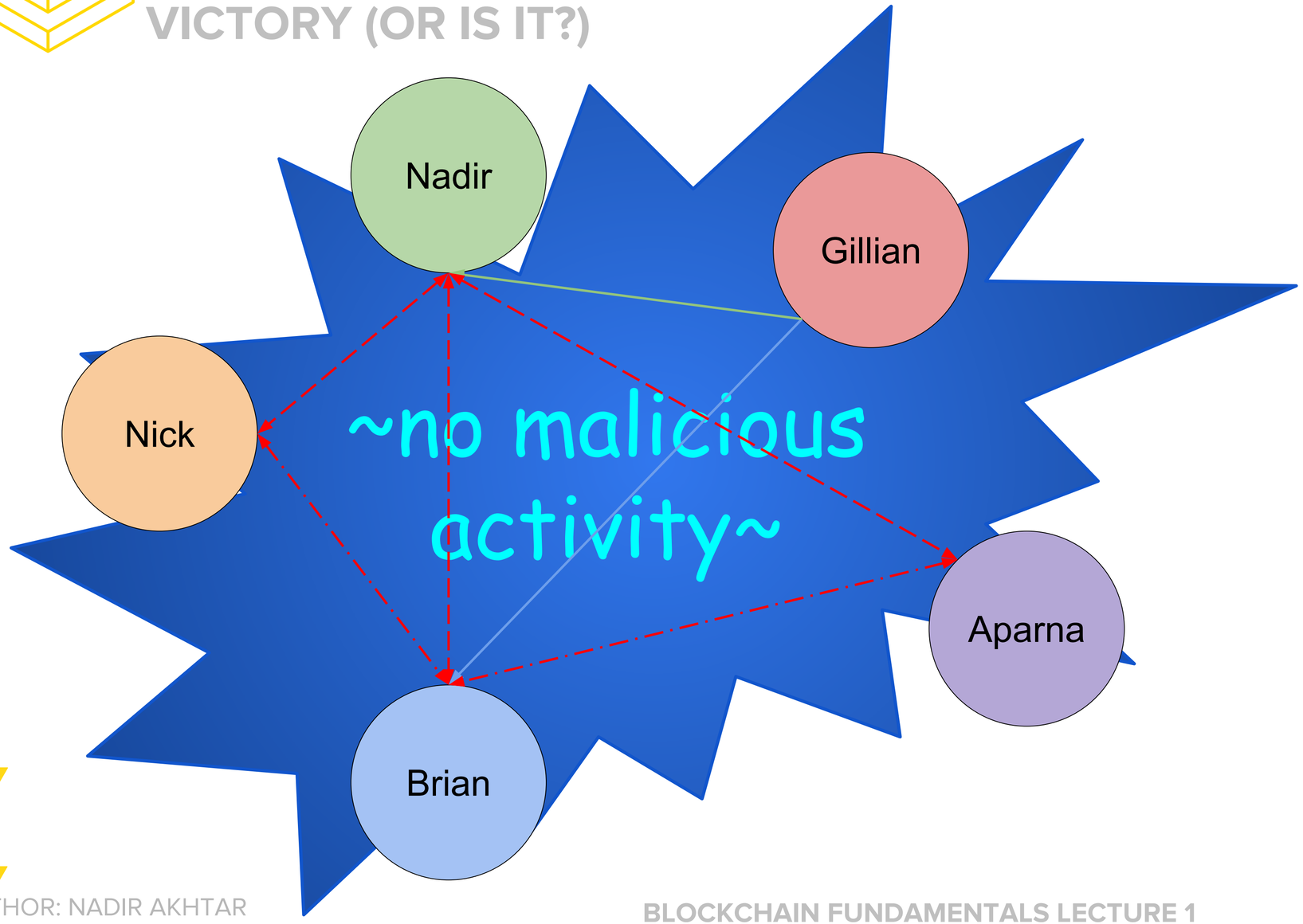
REJECTING THE DOUBLE SPEND



Now, when Gillian attempts to double spend, she will be rejected by observing peers.

CONSENSUS

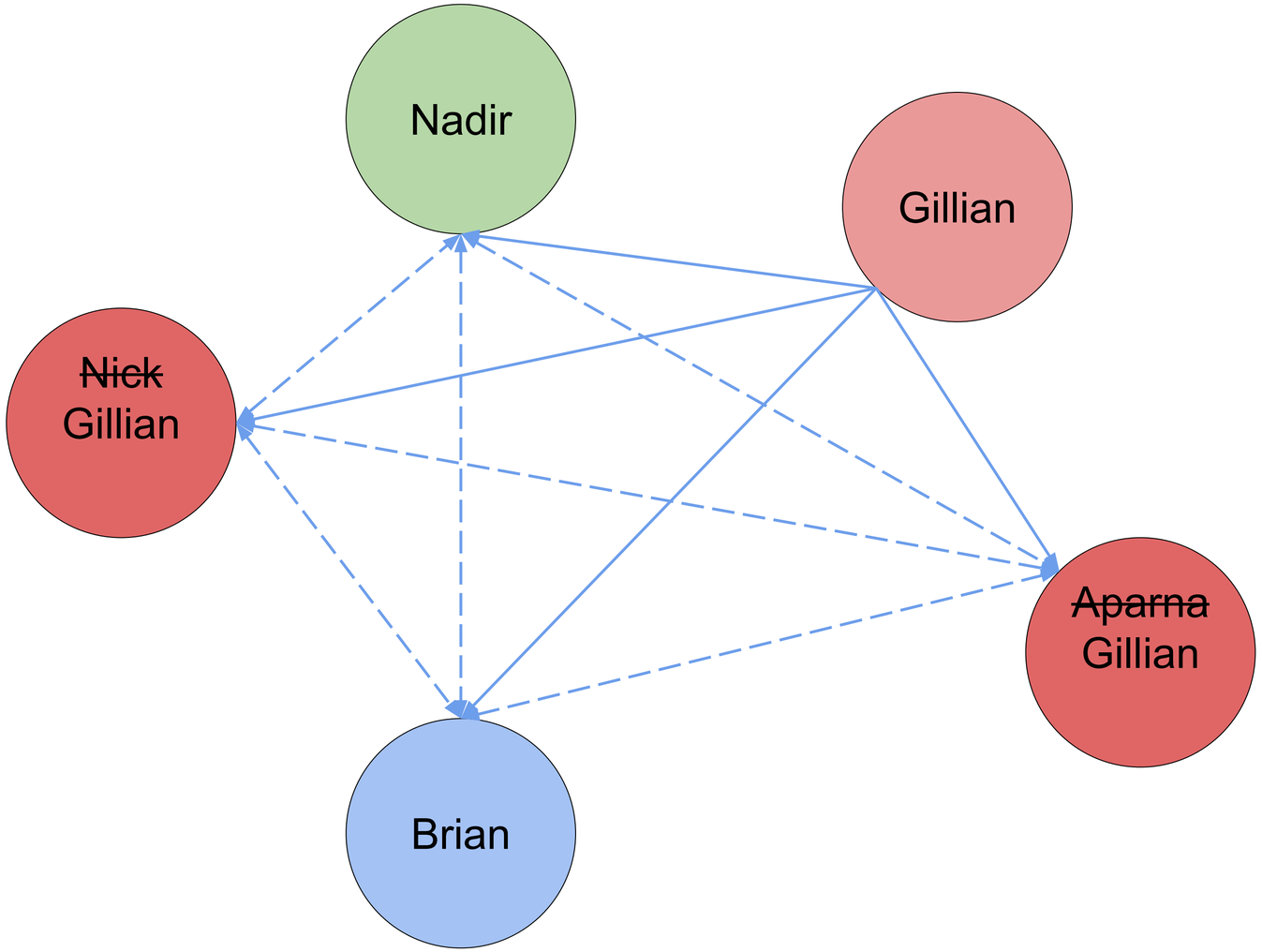
VICTORY (OR IS IT?)



Peers vote “no” on Gillian’s proposal, as they notice multiple transactions trying to spend the same funds.

CONSENSUS

A STRANGER AMONG US

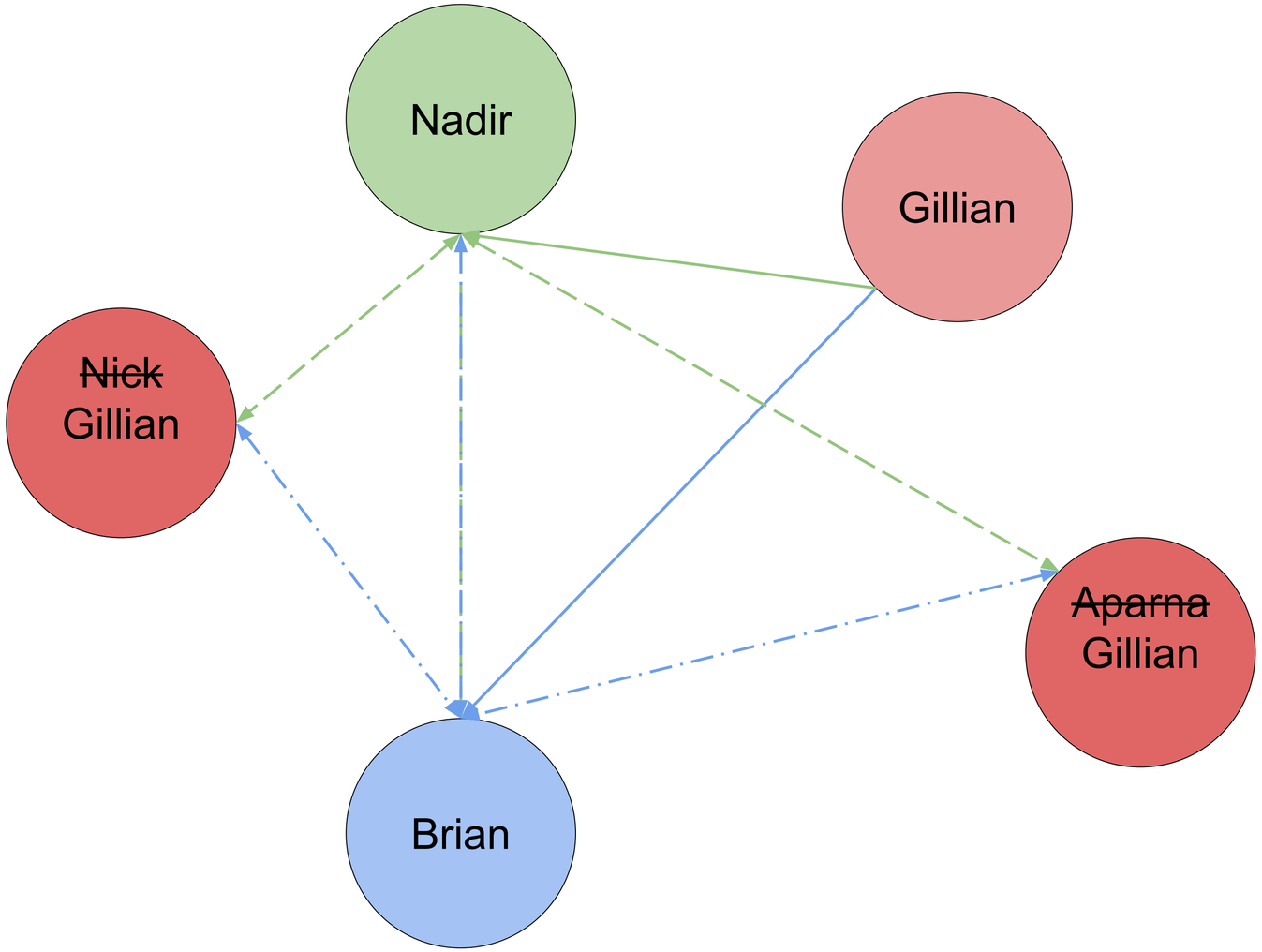


Keep in mind, Bitcoin is an anonymous service with no central registry

- Inexpensive to create multiple identities
- Multiple identities ⇒ multiple opportunities to cast votes

CONSENSUS

A STRANGER AMONG US

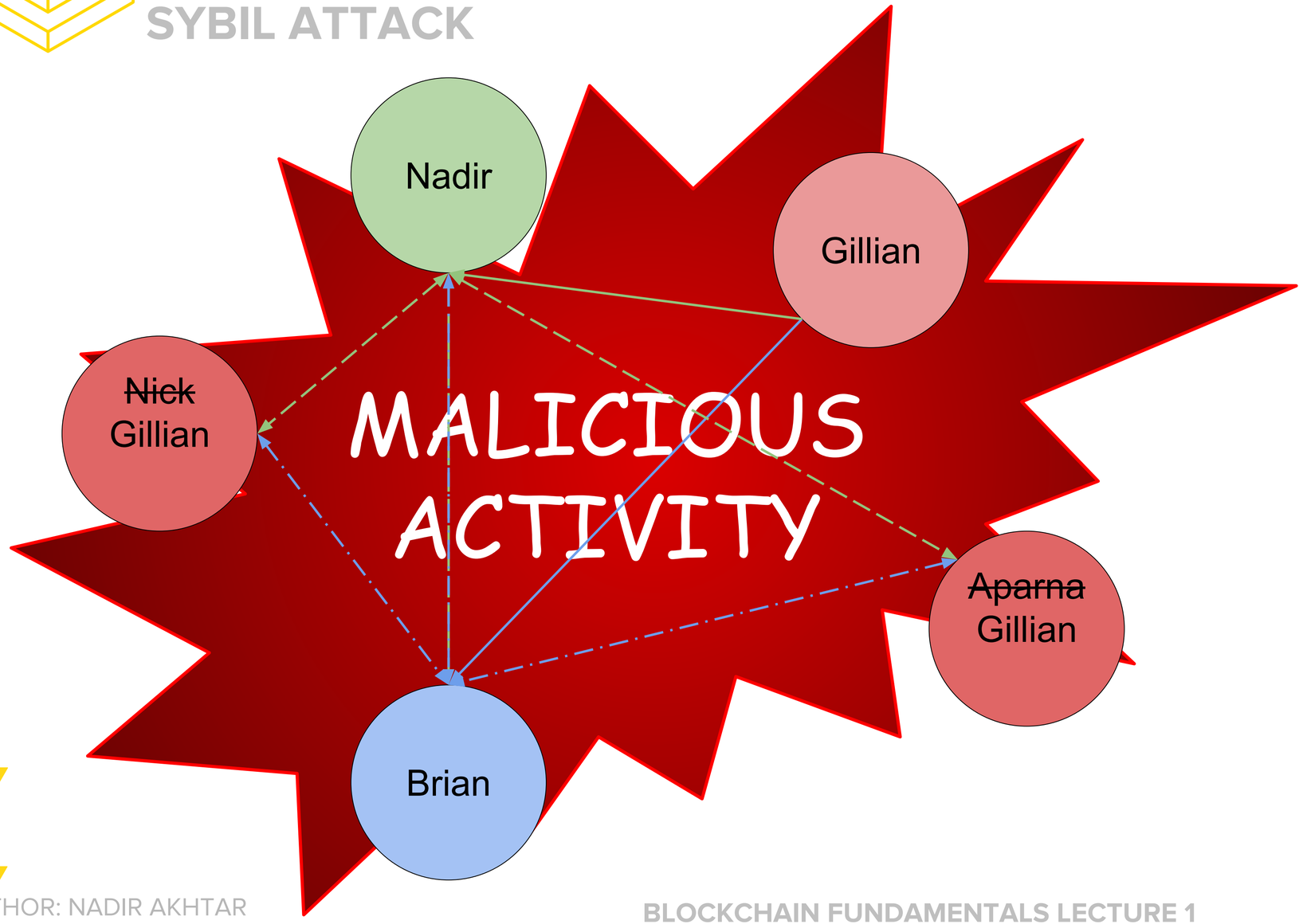


Keep in mind, Bitcoin is an anonymous service with no central registry

- Inexpensive to create multiple identities
- Multiple identities ⇒ multiple opportunities to cast votes

CONSENSUS

SYBIL ATTACK

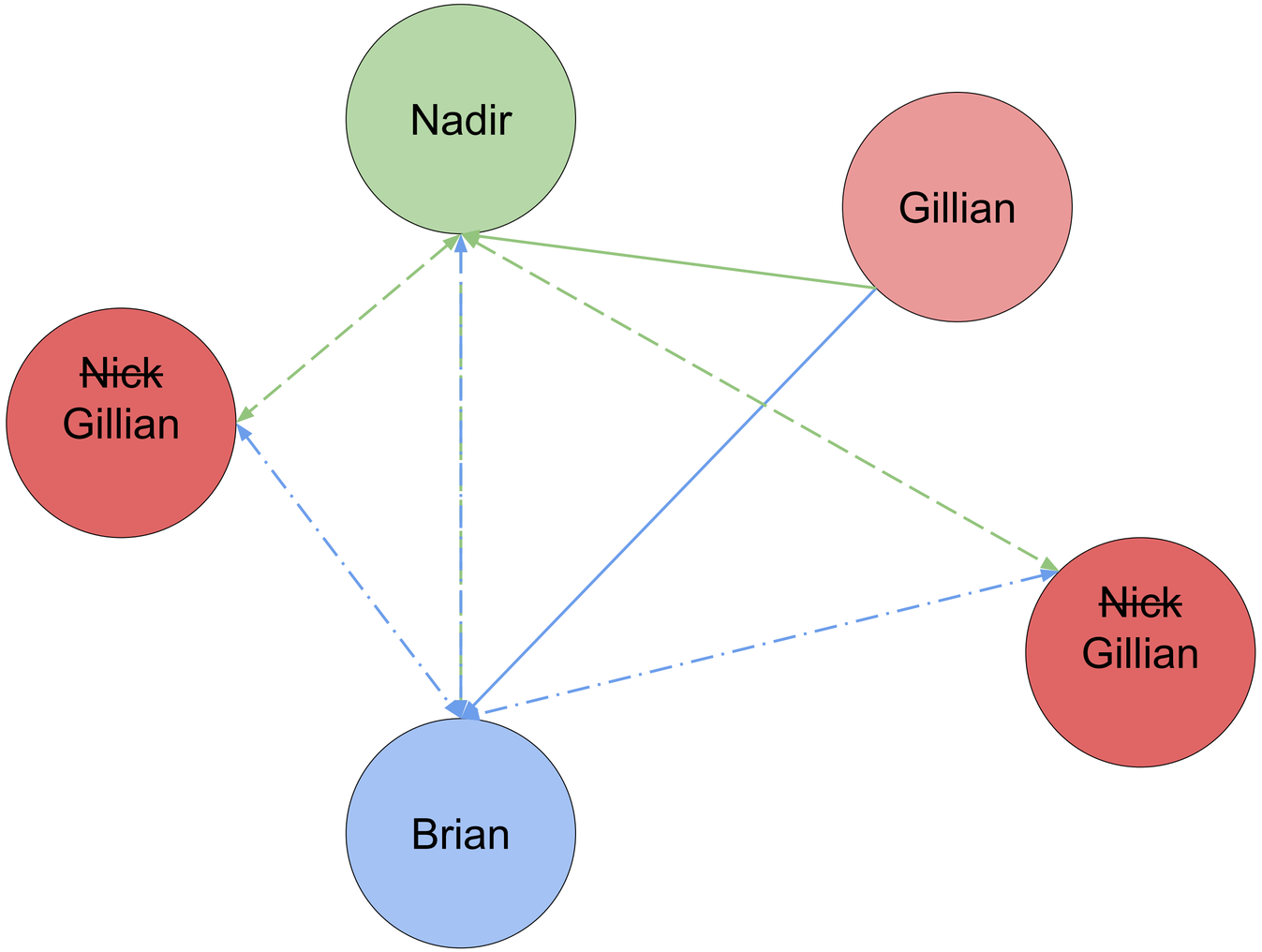


Keep in mind, Bitcoin is an anonymous service with no central registry

- Inexpensive to create multiple identities
- Multiple identities ⇒ multiple opportunities to cast votes
- Gillian can perform a **Sybil attack**, which will allow her to double spend

CONSENSUS

PAY TO PLAY



Instead of casting votes with *identities*, we cast votes with **resources**

CONSENSUS

PROOF-OF-WORK

Proof-of-Work

Evidence

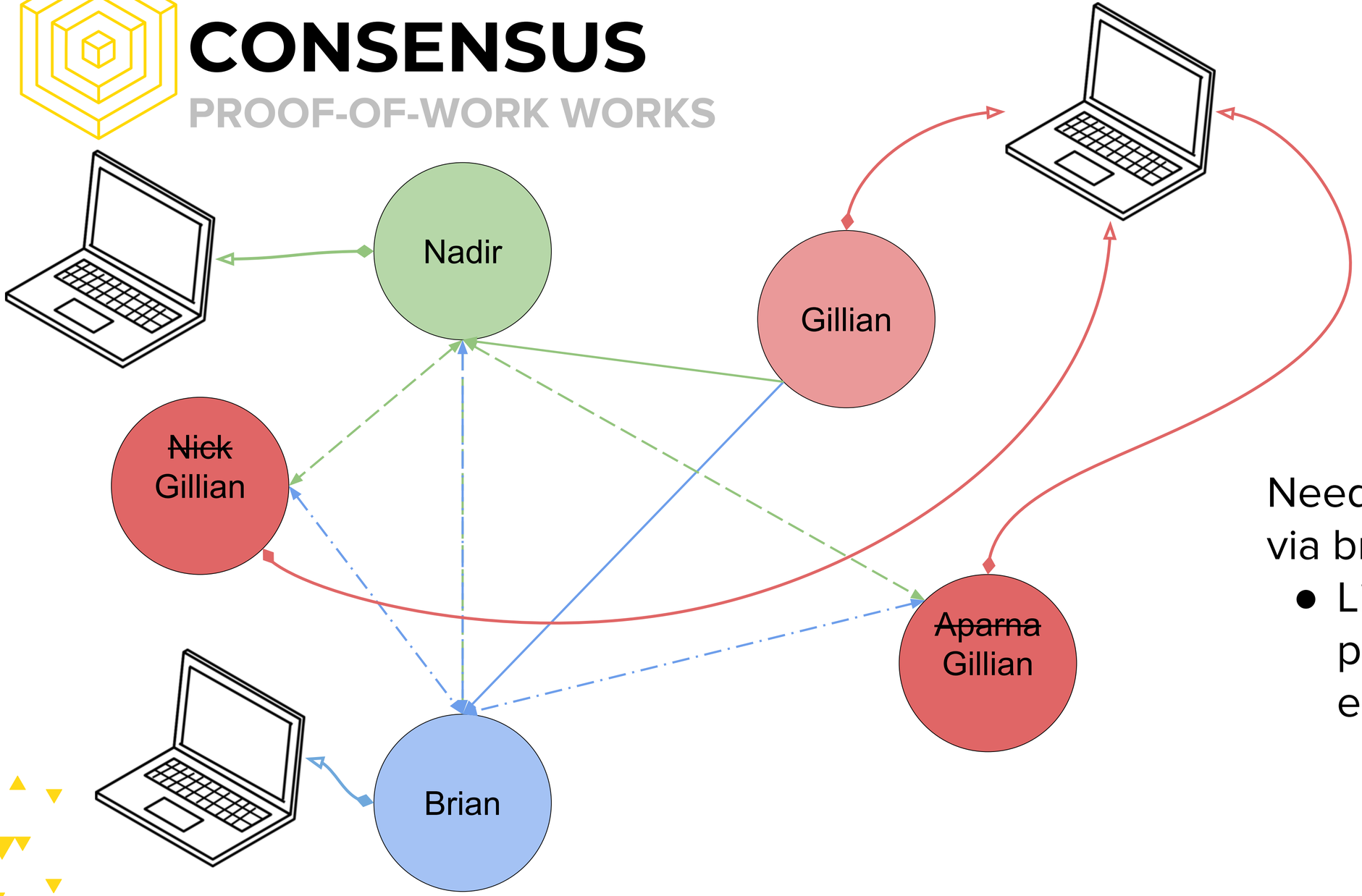
Spent resources

AUTHOR: NADIR AKHTAR

BLOCKCHAIN
AT BERKELEY

CONSENSUS

PROOF-OF-WORK WORKS

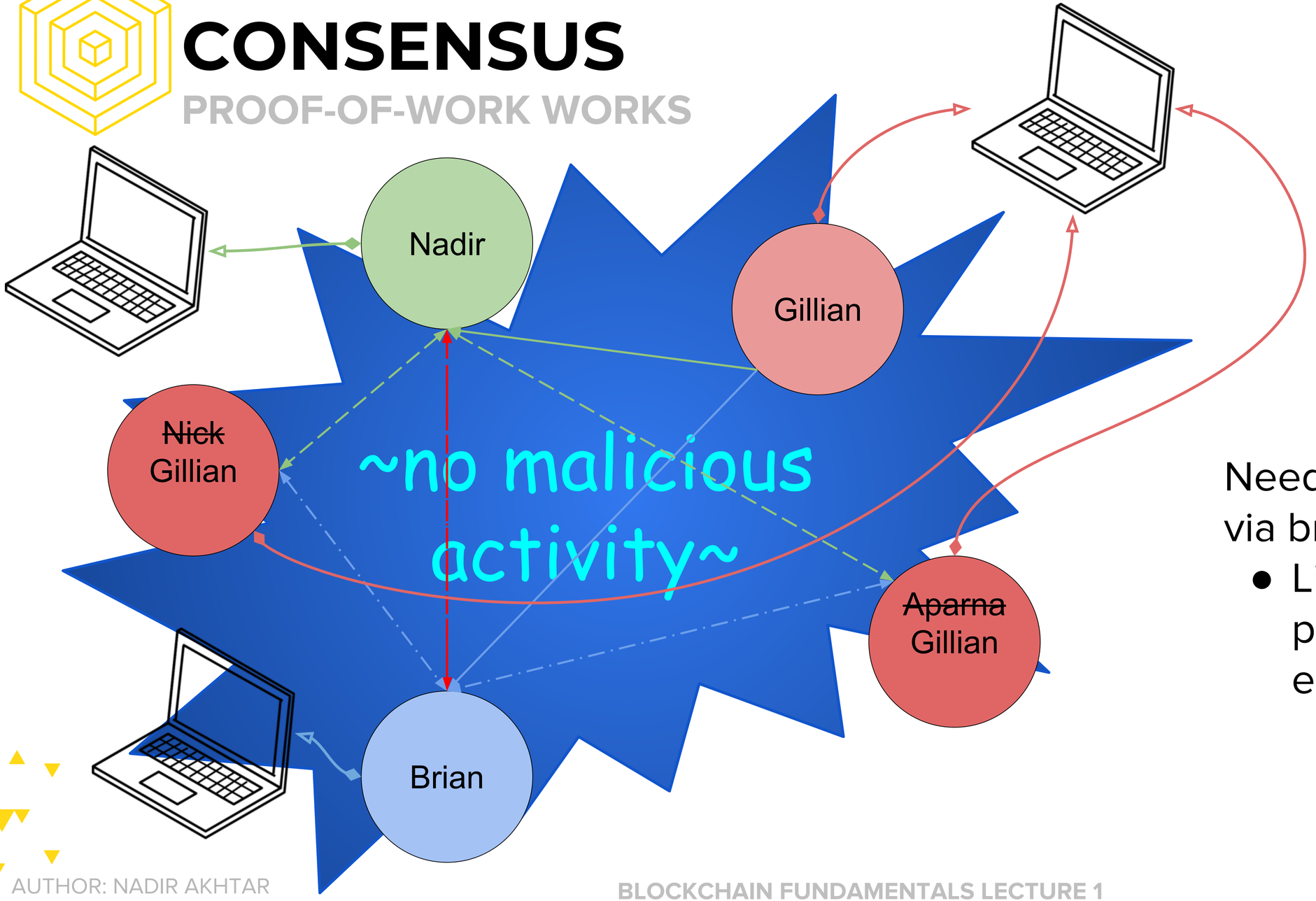


Need to solve a problem via brute forcing

- Like brute forcing a password -- trial and error

CONSENSUS

PROOF-OF-WORK WORKS



Need to solve a problem via brute forcing

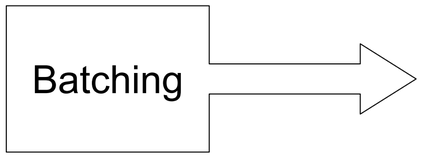
- Like brute forcing a password -- trial and error

QUESTIONS?

EXTRA: FORKING

A LITTLE DIFFERENT FROM SPOONING

Sender	Recipient	Amount (BTC)
Nick	Nadir	0.5
Brian	Gillian	4.2
Aparna	Gillian	23
Gillian	Nick	3.2
Nadir	Brian	0.3
Gillian	Aparna	17



Sender	Recipient	Amount (BTC)
Nick	Nadir	0.5
Brian	Gillian	4.2

Sender	Recipient	Amount (BTC)
Aparna	Gillian	23
Gillian	Nick	3.2

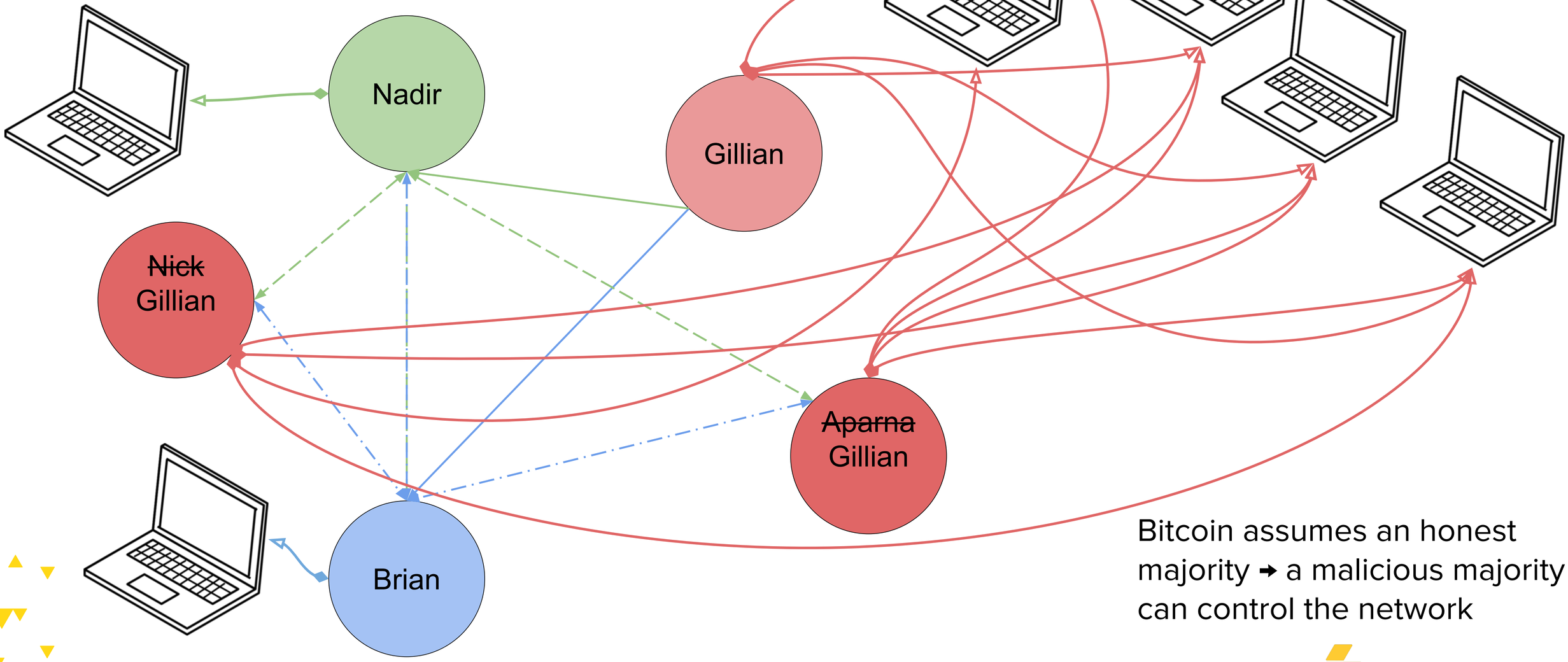
?

Sender	Recipient	Amount (BTC)
Aparna	Gillian	23
Nadir	Brian	0.3

?

EXTRA: 51% ATTACK

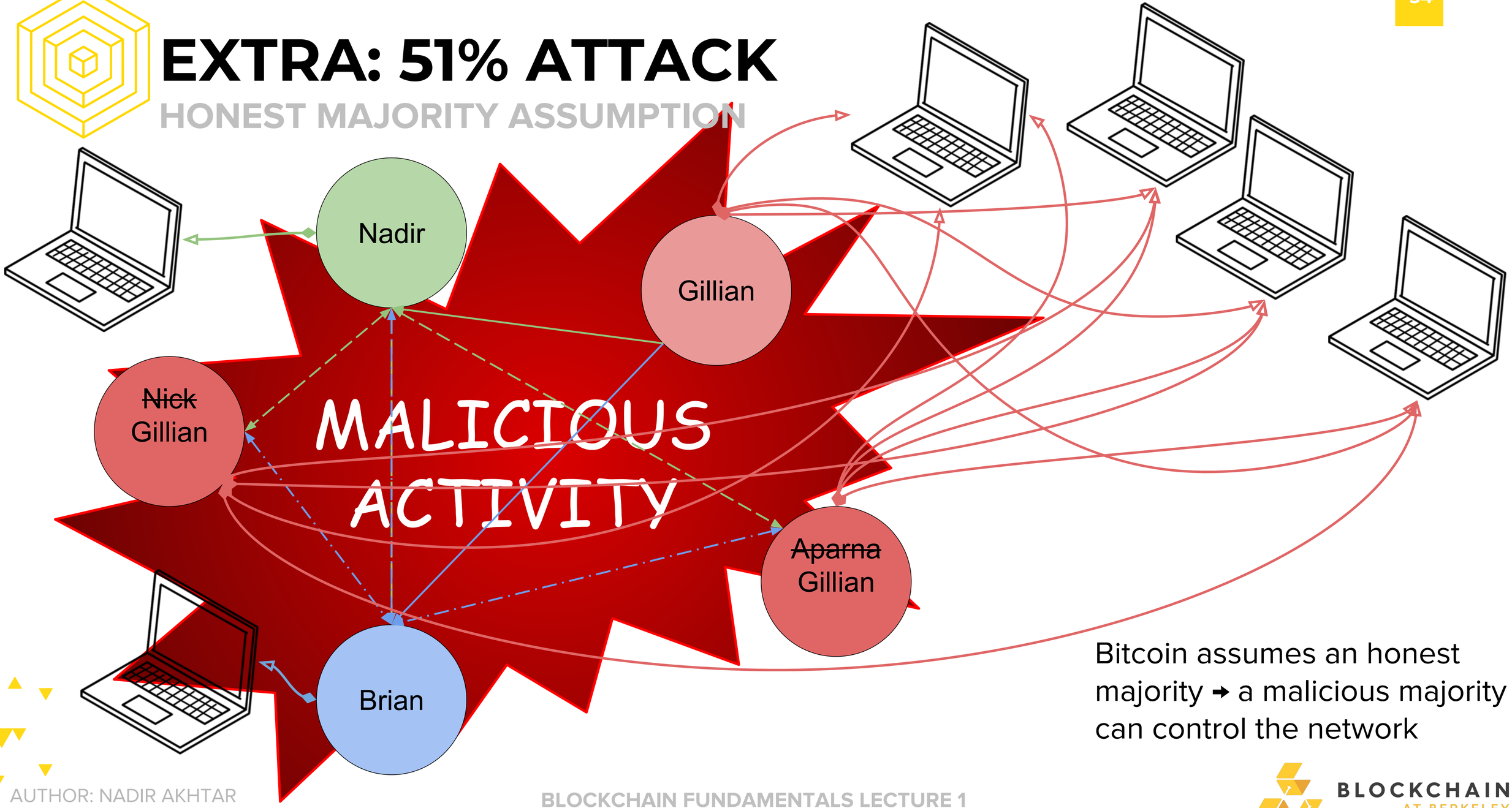
HONEST MAJORITY ASSUMPTION



Bitcoin assumes an honest majority → a malicious majority can control the network

EXTRA: 51% ATTACK

HONEST MAJORITY ASSUMPTION



Bitcoin assumes an honest majority → a malicious majority can control the network

EXTRA: DOUBLE SPENDING

THE ROAD NOT TAKEN

Sender	Recipient	Amount (BTC)
Nick	Nadir	0.5
Brian	Gillian	4.2
Aparna	Gillian	23
Gillian	Nick	3.2
Nadir	Brian	0.3
Gillian	Aparna	17

Batching

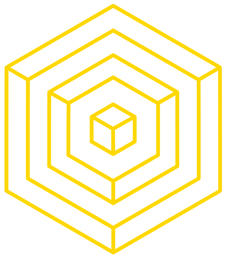
Sender	Recipient	Amount (BTC)
Nick	Nadir	0.5
Brian	Gillian	4.2

Sender	Recipient	Amount (BTC)
Aparna	Gillian	23
Gillian	Nick	3.2

?

Sender	Recipient	Amount (BTC)
Aparna	Gillian	23
Gillian	Gillian	3.2

Sender	Recipient	Amount (BTC)
Nadir	Brian	0.3
Gillian	Aparna	17



REVIEW

SUMMING UP BITCOIN

Identity: We share our public key to transfer Bitcoin and use our private key to redeem it.

Transactions: Under the UTXO model, balances are implicitly the summation of all unspent transaction outputs which you can redeem.

Record-keeping: Each entity keeps a copy of the blockchain, the distributed ledger.

Consensus: Peers cast proposals via Proof-of-Work, an expensive voting process, to deter double spend attacks.

REVIEW

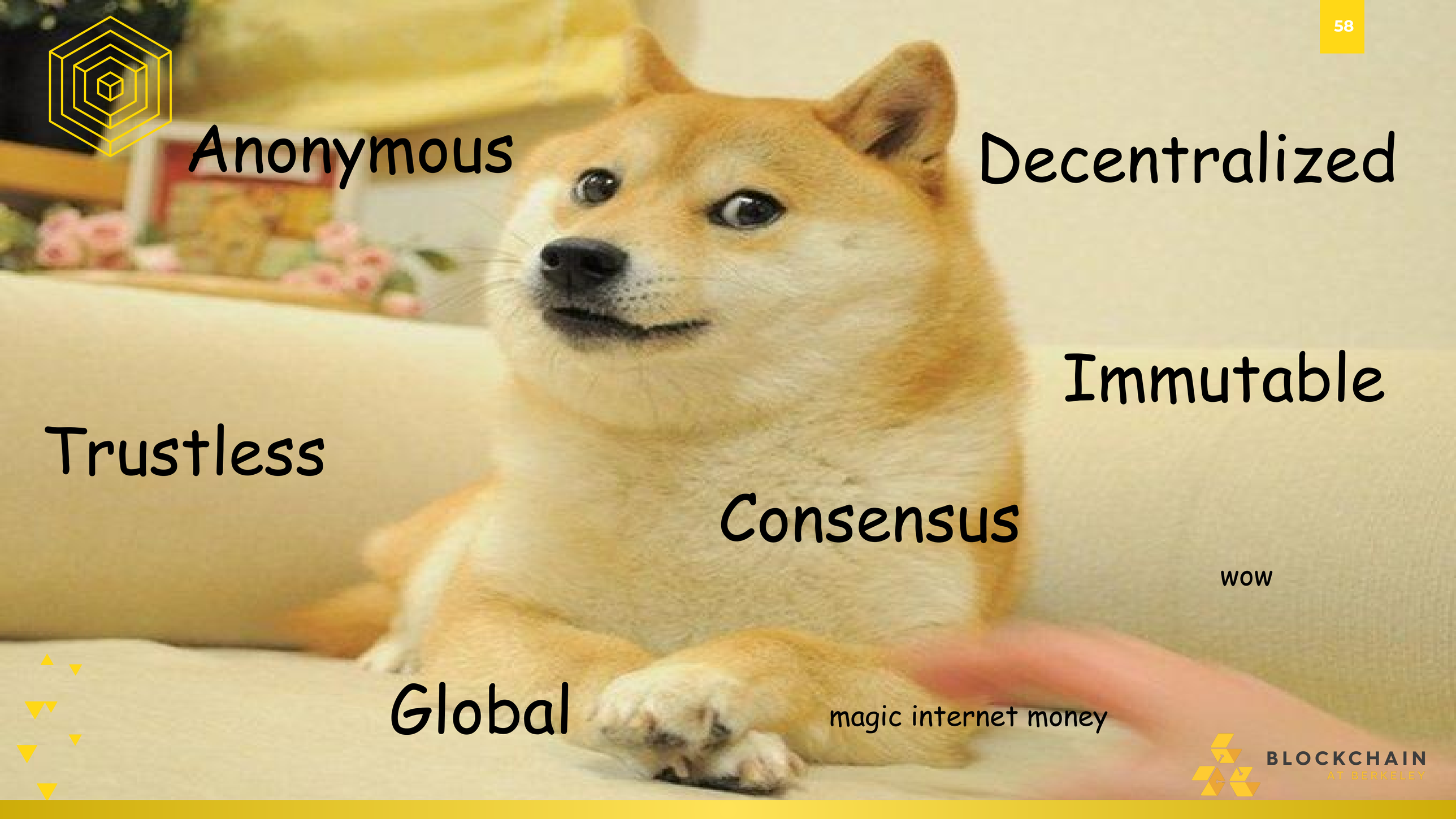
GOALS OF CURRENCY

Source: https://eleventhirthypm.wordpress.com/2013/11/10/the-five-properties-of-currency-not-money/

Currency aims to provide:

- Scarcity: finite units, for maintaining value
- Fungibility: interchangeable and identical units, for preserving equal value between all units
- Divisibility: subunits for every major unit, for ease and precision of payments
- Durability: long-lasting units, for longevity of each unit
- Transferability: liquidity, for ease in transacting

But most importantly, **legitimacy** -- we've demonstrated how we can trust Bitcoin, the mathematical accumulation of several years of research, without trusting individuals.


Anonymous
Decentralized
Immutable
Trustless
Consensus
wow
Global
magic internet money

REVIEW

FINAL WORDS

Source: https://eleventhirthypm.wordpress.com/2013/11/10/the-five-properties-of-currency-not-money/

Questions to think about:

- How well does Bitcoin meet the definition for:
  - A store of value?
  - A unit of account?
  - A medium of exchange?
- How many people do you know that think of Bitcoin as a market cap before technology?
- Can you now explain Bitcoin to your grandma?

QUESTIONS?

HOMEWORK

- **sign up** for Piazza: piazza.com/berkeley/spring2018/compsci19878
- **check out** our syllabus to get an idea of course structure and policy
- **attend** discussion section and use your code to enroll in the right class
  - your code is single-use only and will expire on Feb 2
- **read** the assigned readings posted on Piazza
- **bring** an article to discussion!
- **teach** a friend about how Bitcoin works and/or what it means for the world as best as you can. Some ideas for people to talk to:
  - Roommates
  - Family (Grandmas especially -- they'll feel so smart and tech savvy!)
  - Pets
  - Rubber Ducks
  - RAs
  - Those random AFX teams that manage to pop up everywhere