Secure Systems Engineering: Introductory Comments – Day 2

Bryan Ford
Ecole Polytechnique Federale de Lausanne (EPFL)

http://bford.info/

FOSAD – Bertinoro, Italy – August 30, 2016

The Story Thus Far…

- Intro: Systems, Distributed/Decentralized
- “Provable security” must connect to real users
  - e.g., USENET: censor-proof, but died from spam
- Dissent: stab at practical, provable anonymity
- Dissent in Numbers: scaling from 10s to 1000s
- Collective Control Plane: resists active attacks
- Buddies: (attempt to) resist intersection attacks
  - Positive: working mechanisms to measure, control
  - Negative: serious anonymity/availability tradeoffs

Explosion of interest in building "provable anonymity systems"

- **Dissent** – Wolinsky et al, CCS 10, OSDI 2012
- **Aqua** – Le Blond et al, SIGCOMM 2013
- **CoinShuffle** – Ruffing et al, ESORICS 2014
- **Riposte** – Corrigan-Gibbs et al, Oakland 2015
- **Baffle** – Zamani et al, ICDCS 2015
- **Herd** – Le Blond et al, SIGCOMM 2015
- **Vuvuzela** – van den Hoof, SOSP 2015
- **Riffle** – Kwon et al, PETS 2016

Still Many Open Challenges in [Provable] Anonymity Systems

Some key missing puzzle pieces:

- Intersection attacks: is resistance practical?
- Scaling: get from thousands to millions of users
- Provisioning: where do the servers come from?
- Coordination: large-scale trustless agreement
- Incentives: beyond volunteer infrastructure?

Next Up

Puzzle Pieces for Future Decentralized Systems

- **AnonRep:** reputation instead of pseudonyms?
- **Cothorities:** scalable collective authorities
- **RandHound:** random coins, random groups
- **ByzCoin:** large-scale consensus, coinage
- **Pseudonym Parties:** the fake people problem

Conclusion: into the wild unknown

AnonRep: Towards Tracking-Resistant Anonymous Reputation

Ennan Zhai[1]

David Isaac Wolinsky[2], Ruichuan Chen[3],

Ewa Syta[1], Chao Teng[2], Bryan Ford[4]

[1] *Yale* [2] *Facebook* [3] *Bell Labs* [4] *EPFL*

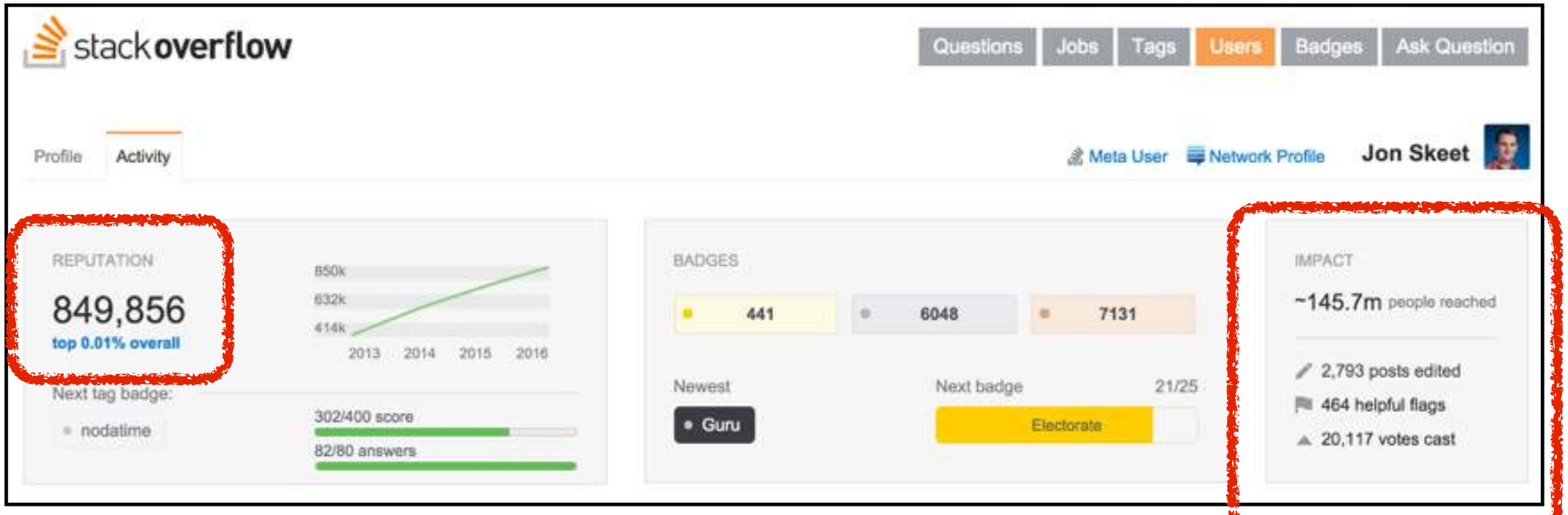
Background

- There is too much information on today's Internet

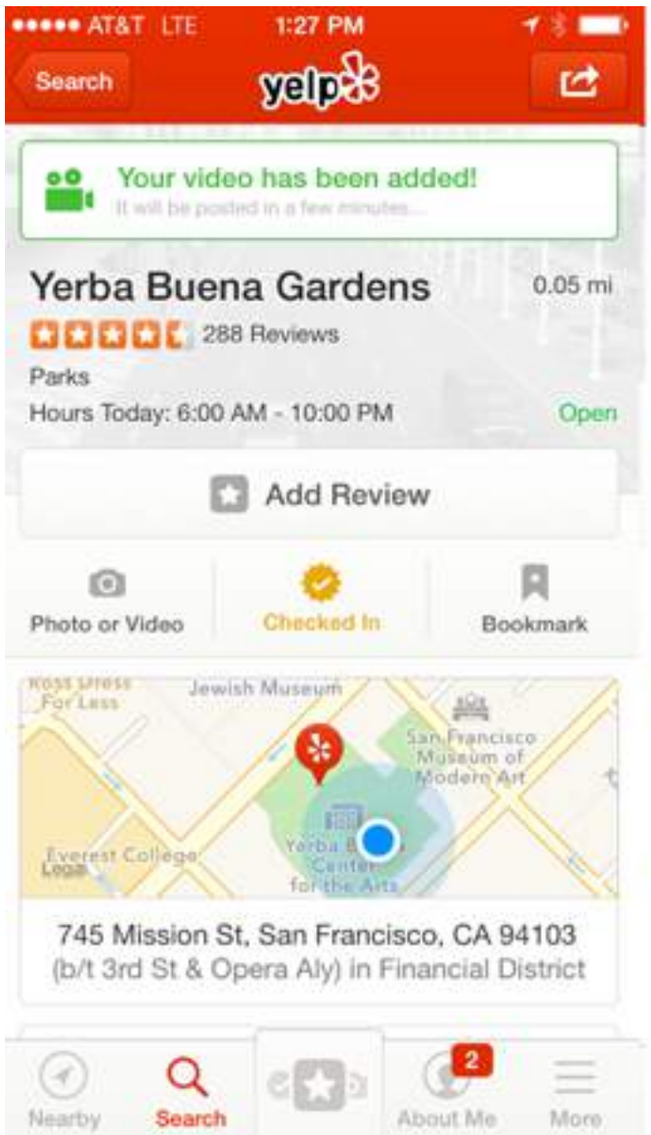
Background

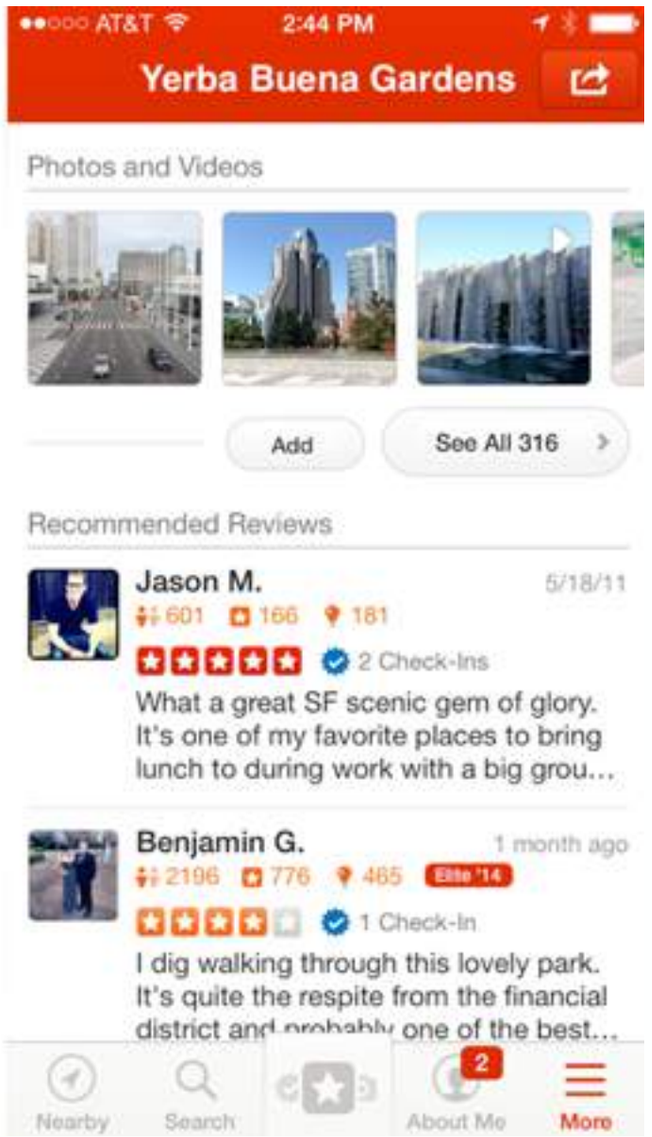
- There is too much information on today's Internet
- Reputation systems are employed:
  - Highlighting information quality
  - Filtering spam

Stack Overflow

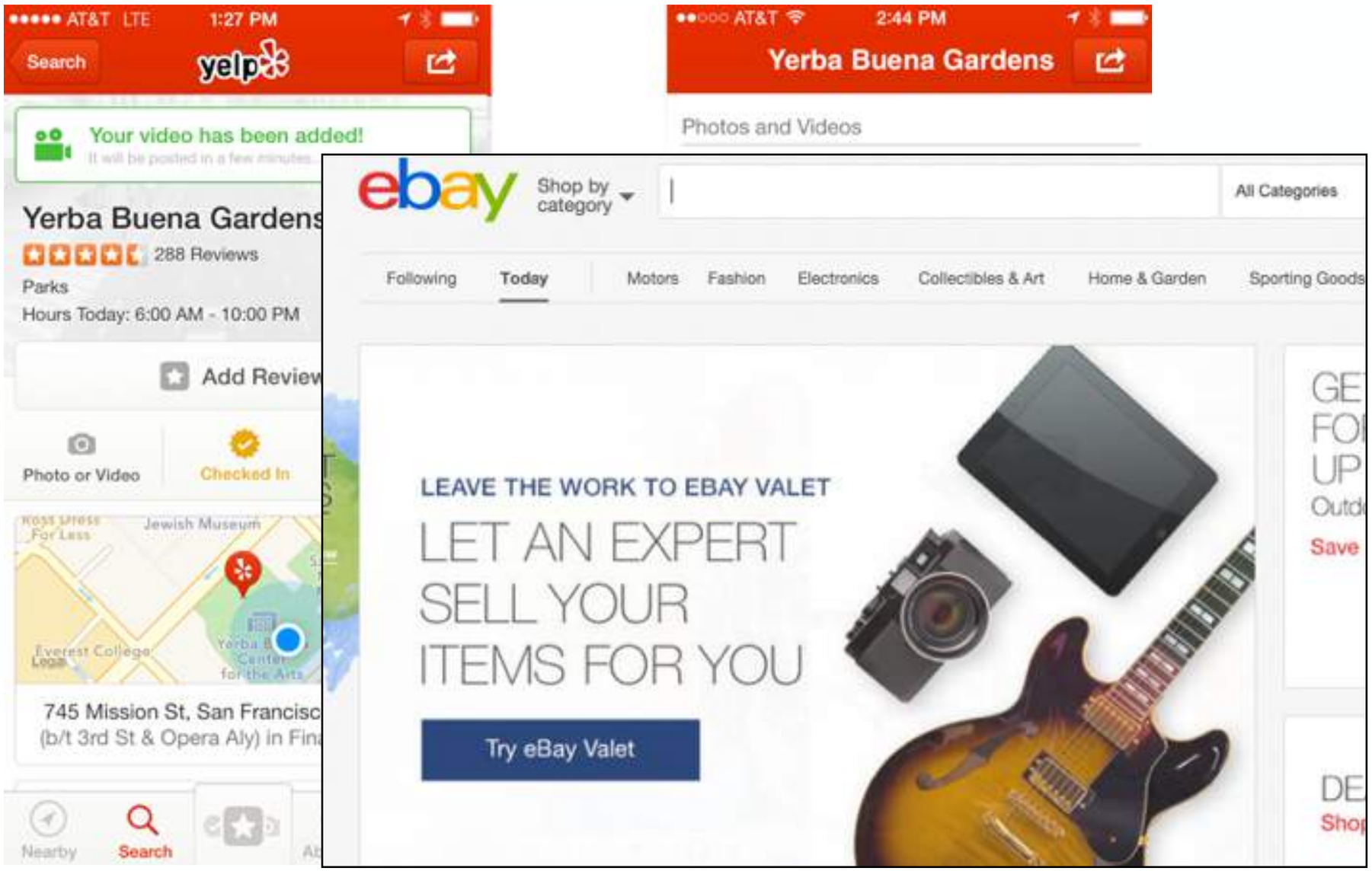


Reputation System

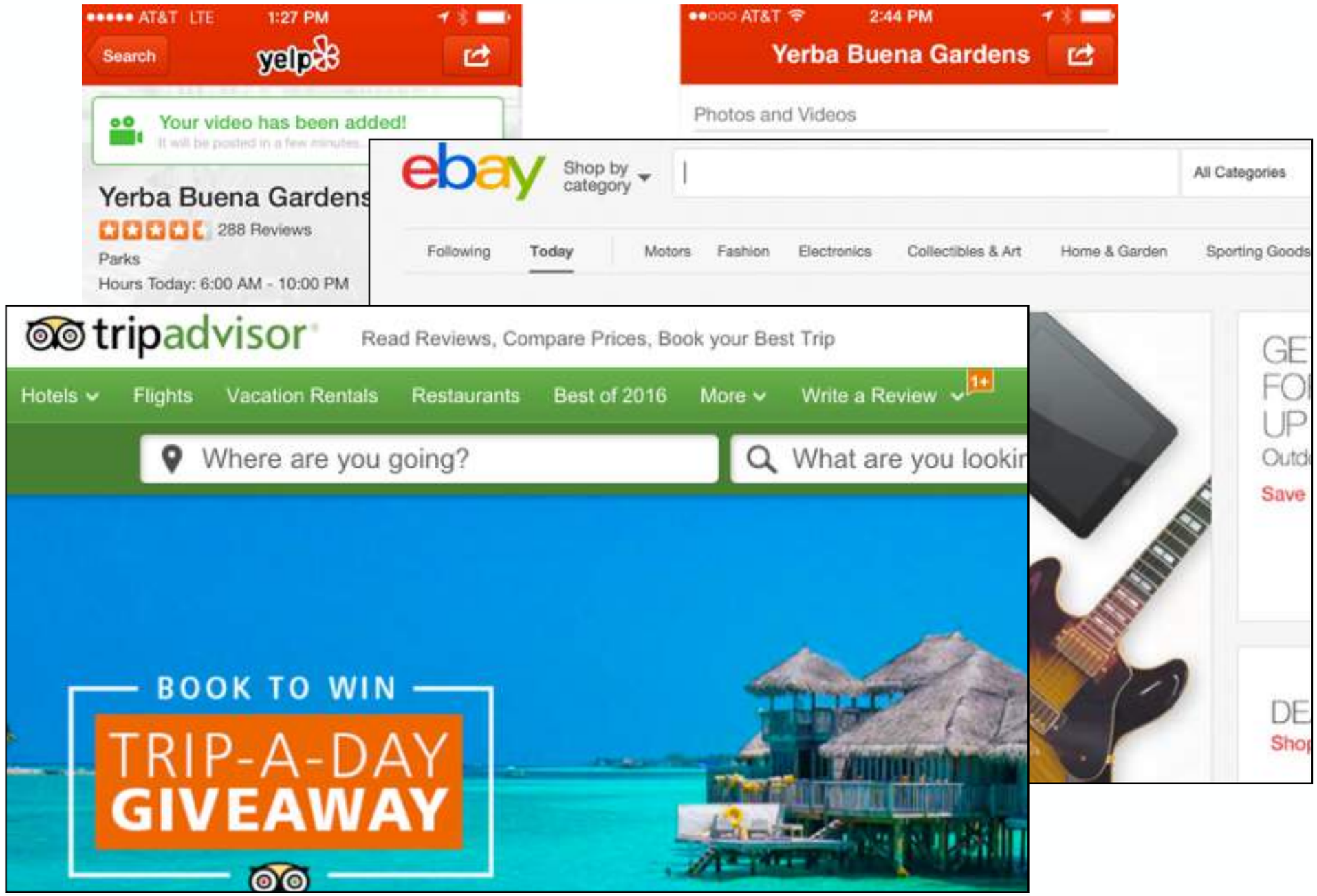




Reputation System



Reputation System



Reputation System

Messages	Author (Score)	Votes
…	…	
…	…	
…	…	
…	…	

Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (0)	0
…	…	
…	…	
…	…	

Reputation System

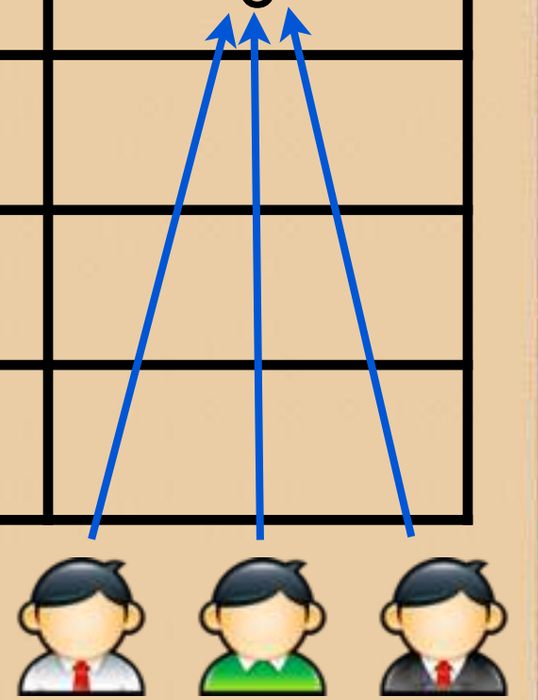
Messages	Author (Score)	Votes
I like NSDI'16	Alice (0)	0
…	…	
…	…	
…	…	

Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (0)	0
…	…	
…	…	
…	…	

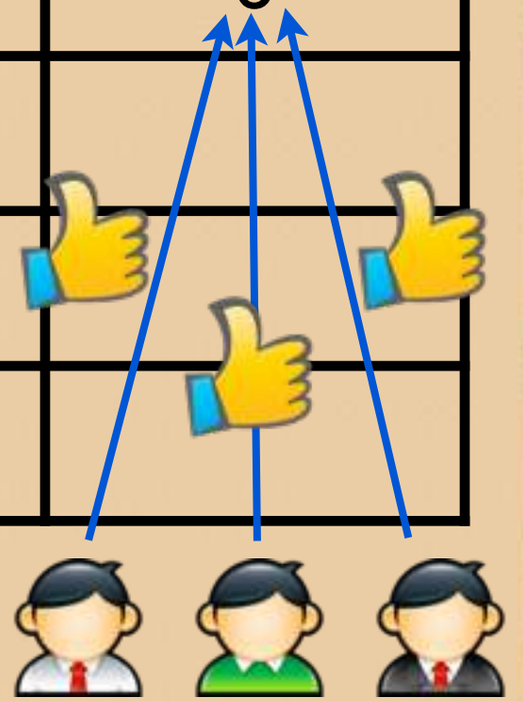
Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (0)	0
…	…	
…	…	
…	…	



Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (0)	0
…	…	
…	…	
…	…	



Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (0)	Like: 3
…	…	
…	…	
…	…	

Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
…	…	
…	…	
…	…	

$\sum V_i = 1+1+1 = 3$

Reputation System

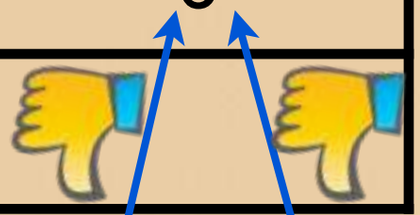
Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
...	...	
...	...	

Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
Yale colleges are bad	Bob (1)	0
...	...	

Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
Yale colleges are bad	Bob (1)	0
...	...	



Alice Dave

Reputation System

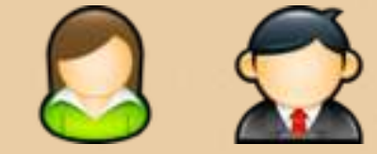
Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
Yale colleges are bad	Bob (1)	Dislike: 2
...	...	

Alice Dave

Reputation System

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
Yale colleges are bad	Bob (-1)	Dislike: 2
...	...	

$\sum V_i = 1-1-1 = -1$



People Care About Privacy

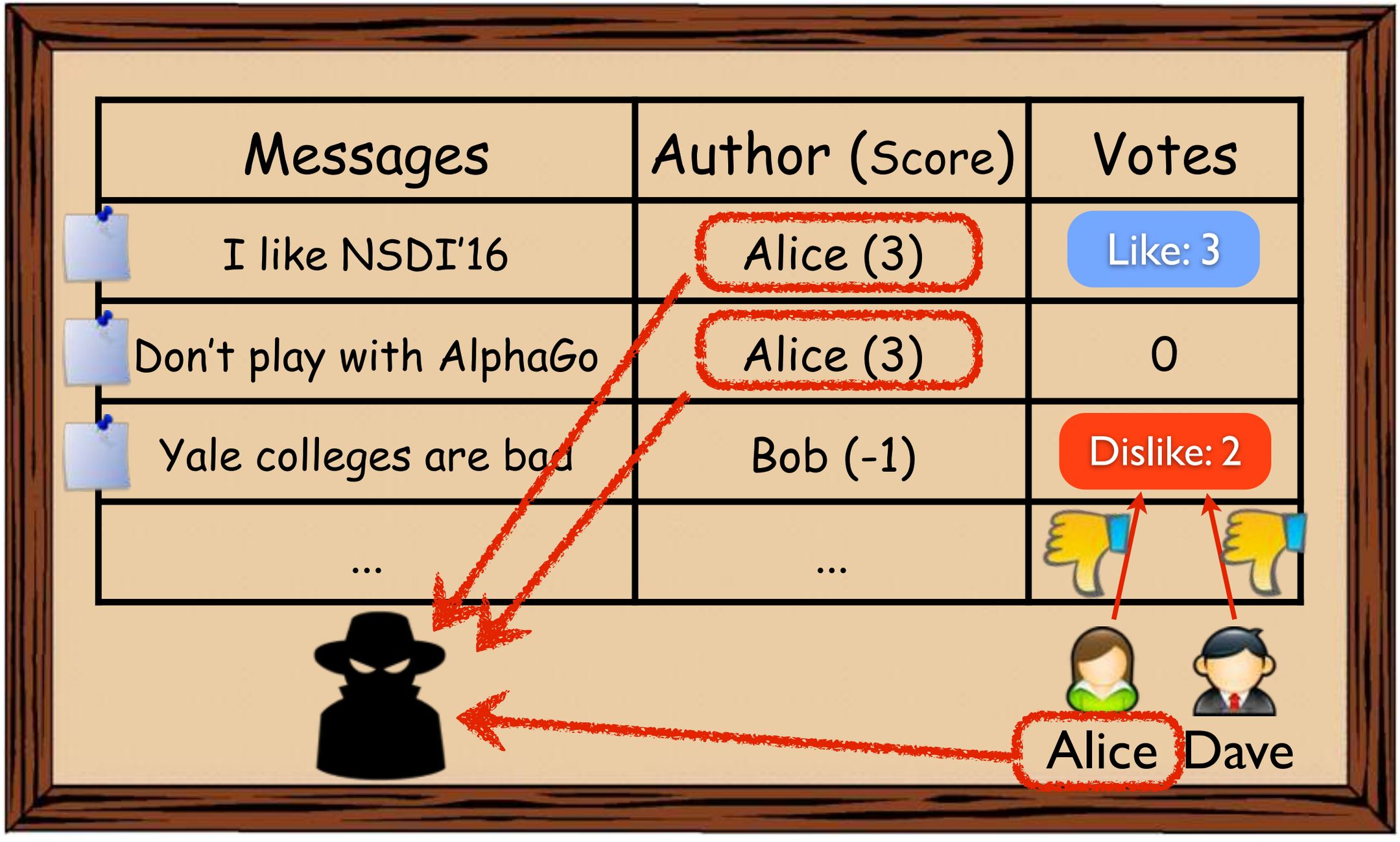
- People want to participate in these reputation systems **anonymously** :
  - Sensitive topics
  - Business competitions
  - Other personal concerns

People Care About Privacy

- People want to participate in these re**sly** :
  - S
  - B
  - C

TARGET: Linkability Problem

TARGET: Linkability Problem



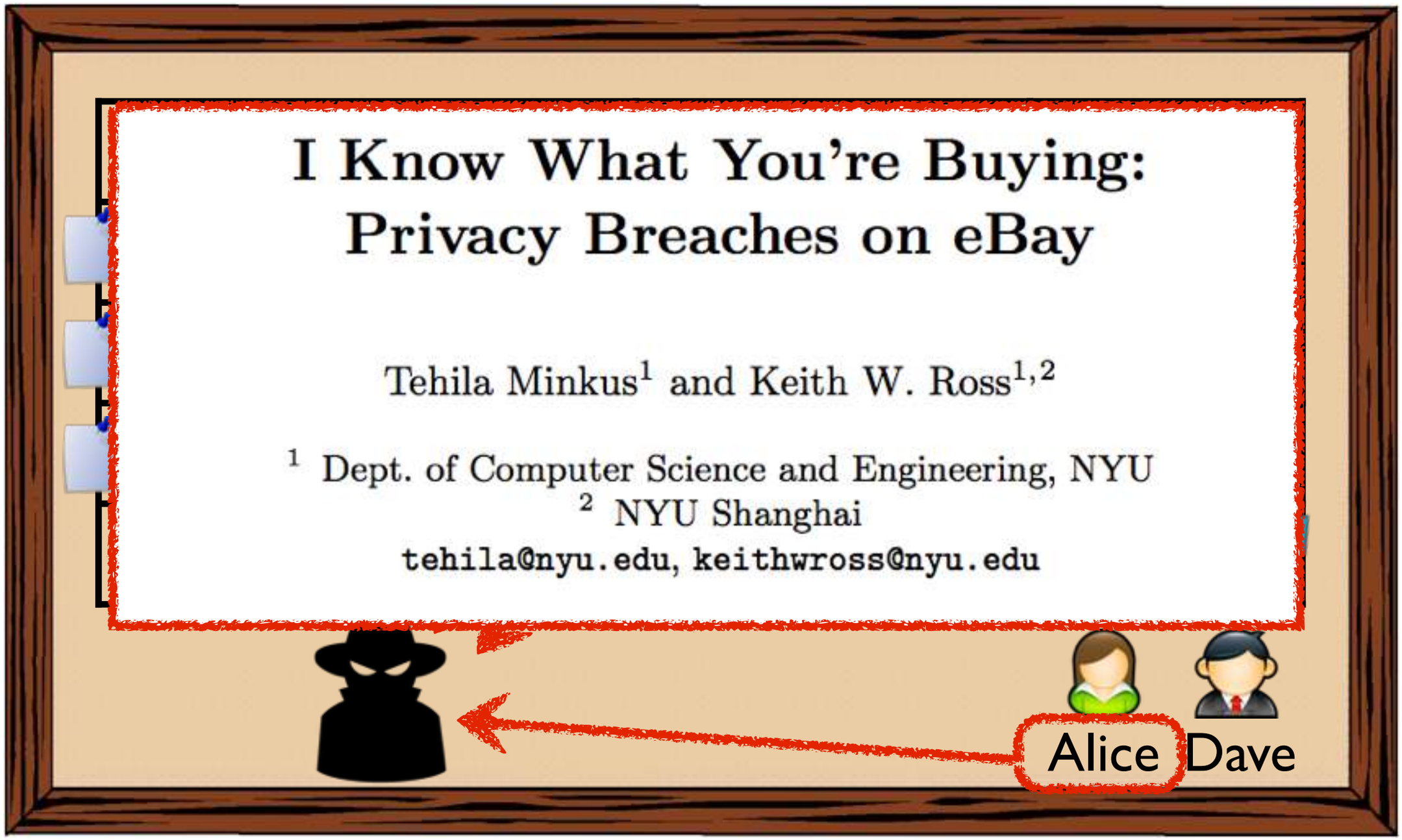
TARGET: Linkability Problem

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
Yale colleges are bad	Bob (-1)	Dislike: 2
...	...	

Alice Dave

Reputation system provider

TARGET: Linkability Problem



Anonymous Reputation System

Reputation system provider and **any user** should not be able to link any user's activities

Existing Efforts

- E-Cash based approaches [1]:
  - Only support positive feedback
  - Not support diverse reputation algorithms

[1] John Bethencourt et al. Signatures of reputation. In FC'10.

Existing Efforts

- E-Cash based approaches [1]:
  - Only support positive feedback
  - Not support diverse reputation algorithms

- Blind signature-based efforts [2]:
  - Also limited to positive feedback
  - Need a centralized banker

[1] John Bethencourt et al. Signatures of reputation. In FC'10.

[2] Elli Androulaki et al. Reputation systems for anonymous networks. In PETS'08.

Existing Efforts

- E-Cash based approaches [1]:
  - Only support positive feedback
  - Not support diverse reputation algorithms

- Blind signature-based efforts [2]:
  - Also limited to positive feedback
  - Need a centralized banker

The primitives they depend on are computationally expensive!

[1] John Bethencourt et al. Signatures of reputation. In FC'10.

[2] Elli Androulaki et al. Reputation systems for anonymous networks. In PETS'08.

Our Goals

- Tracking-resistant anonymous reputation:
  - Unlinkability and anonymity of users' activities
  - Diverse reputation utilities (algorithms)

Our Goals

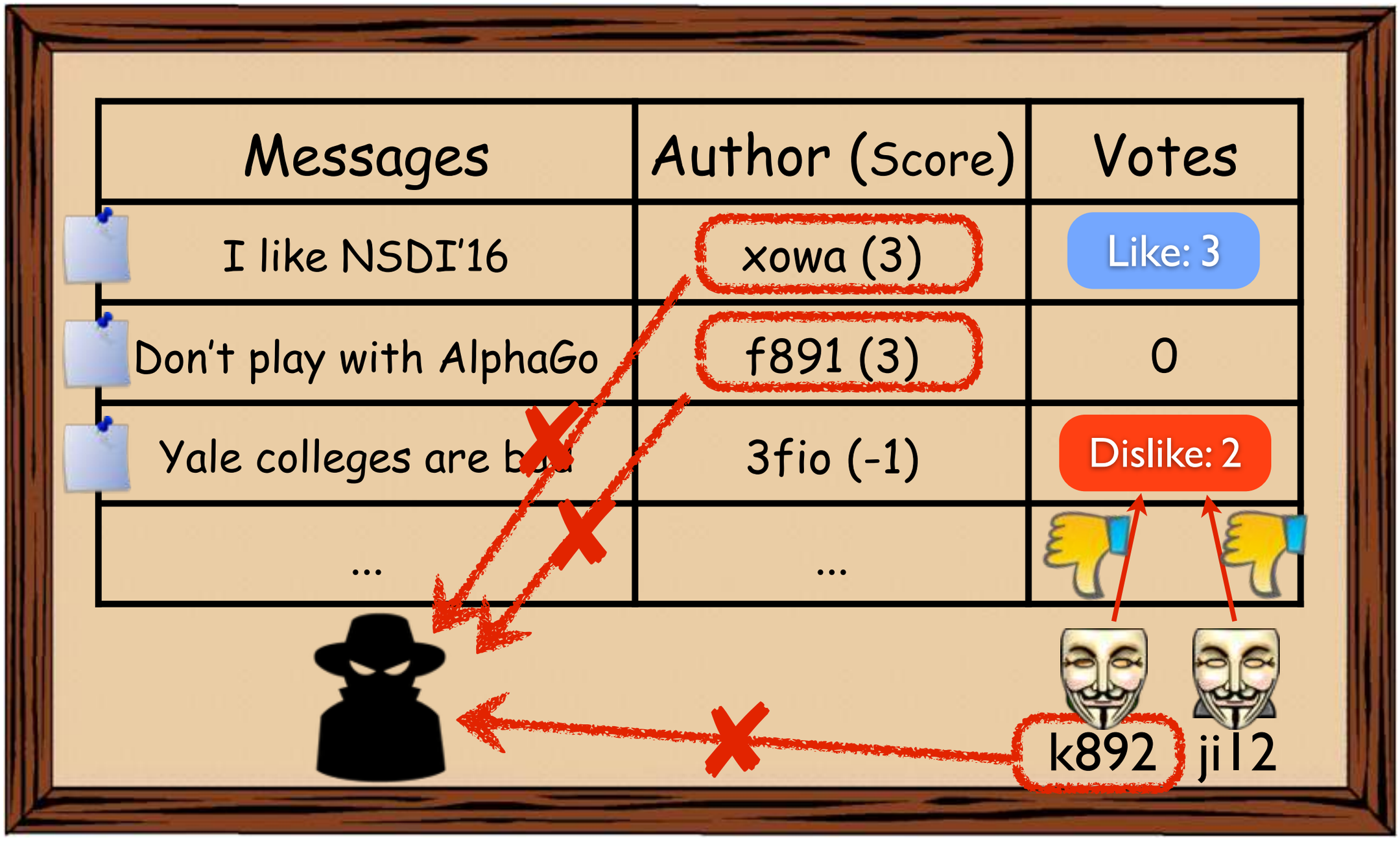
- Tracking-resistant anonymous reputation:
  - Unlinkability and anonymity of users' activities
  - Diverse reputation utilities (algorithms)
  - No need trust any centralized party
  - Scalable to large-size user set

Example

Messages	Author (Score)	Votes
I like NSDI'16	Alice (3)	Like: 3
Don't play with AlphaGo	Alice (3)	0
Yale colleges are bad	Bob (-1)	Dislike: 2
...	...	

Alice Dave

Example


Messages
Author (Score)
Votes
I like NSDI'16
xowa (3)
Like: 3
Don't play with AlphaGo
f891 (3)
0
Yale colleges are b
3fio (-1)
Dislike: 2
...
...
k892
ji12

Technical Challenges

Technical Challenges

- Reputation update relies on activities tracking

It is a paradox in practice!

Technical Challenges

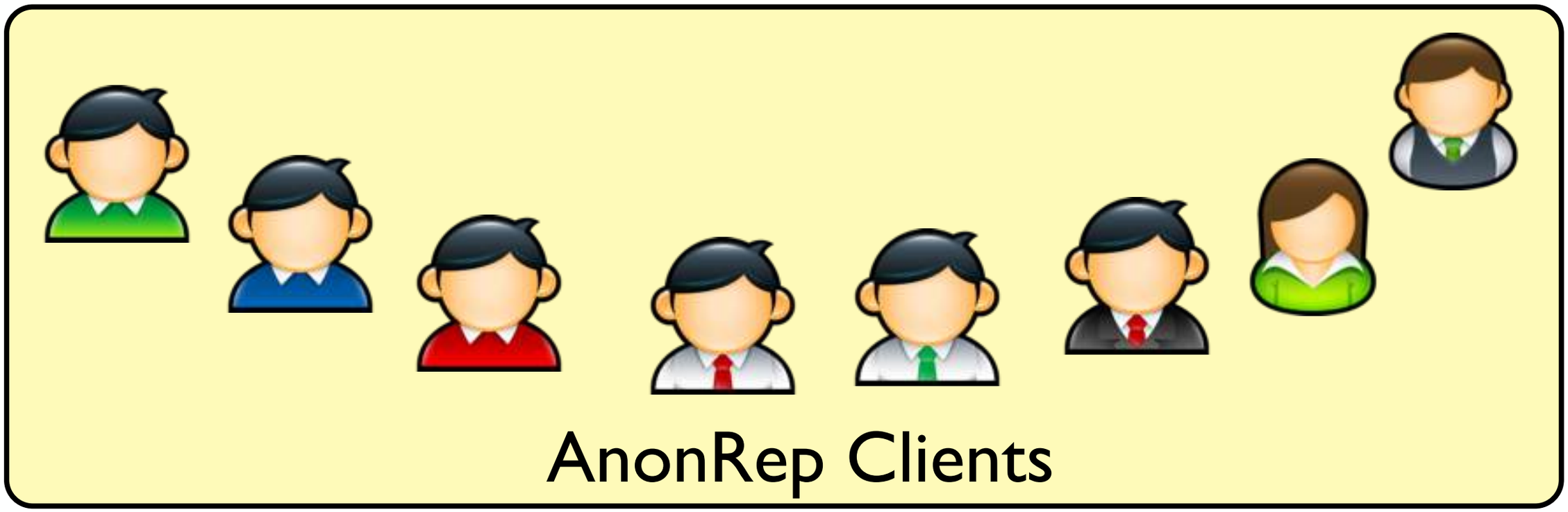
- Reputation update relies on activities tracking
- Misbehaviors (e.g., duplicate voting) detection

Road-Map

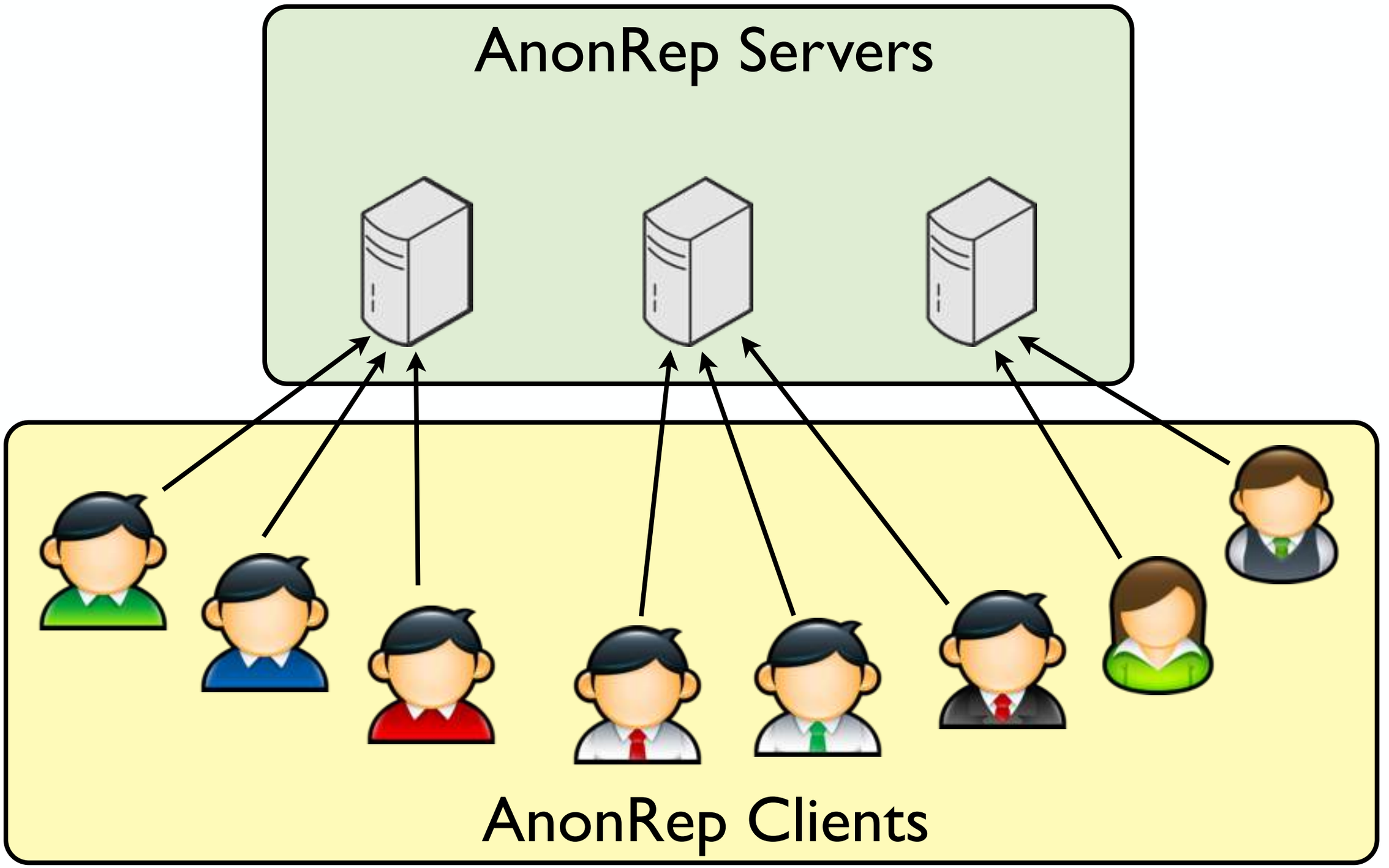
- Motivations
- AnonRep Design
- Practical Considerations
- Evaluation

AnonRep Deployment

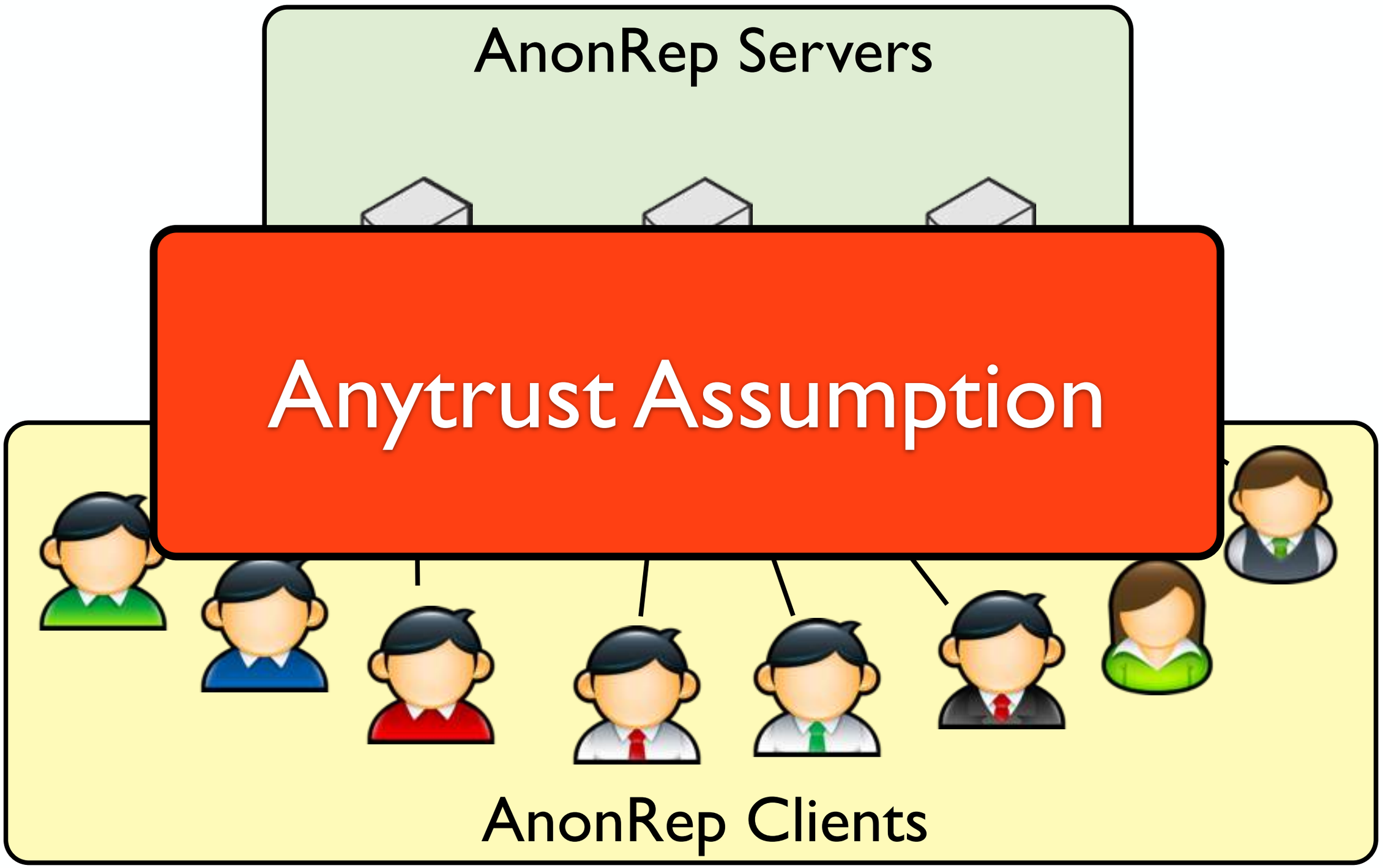
AnonRep Deployment



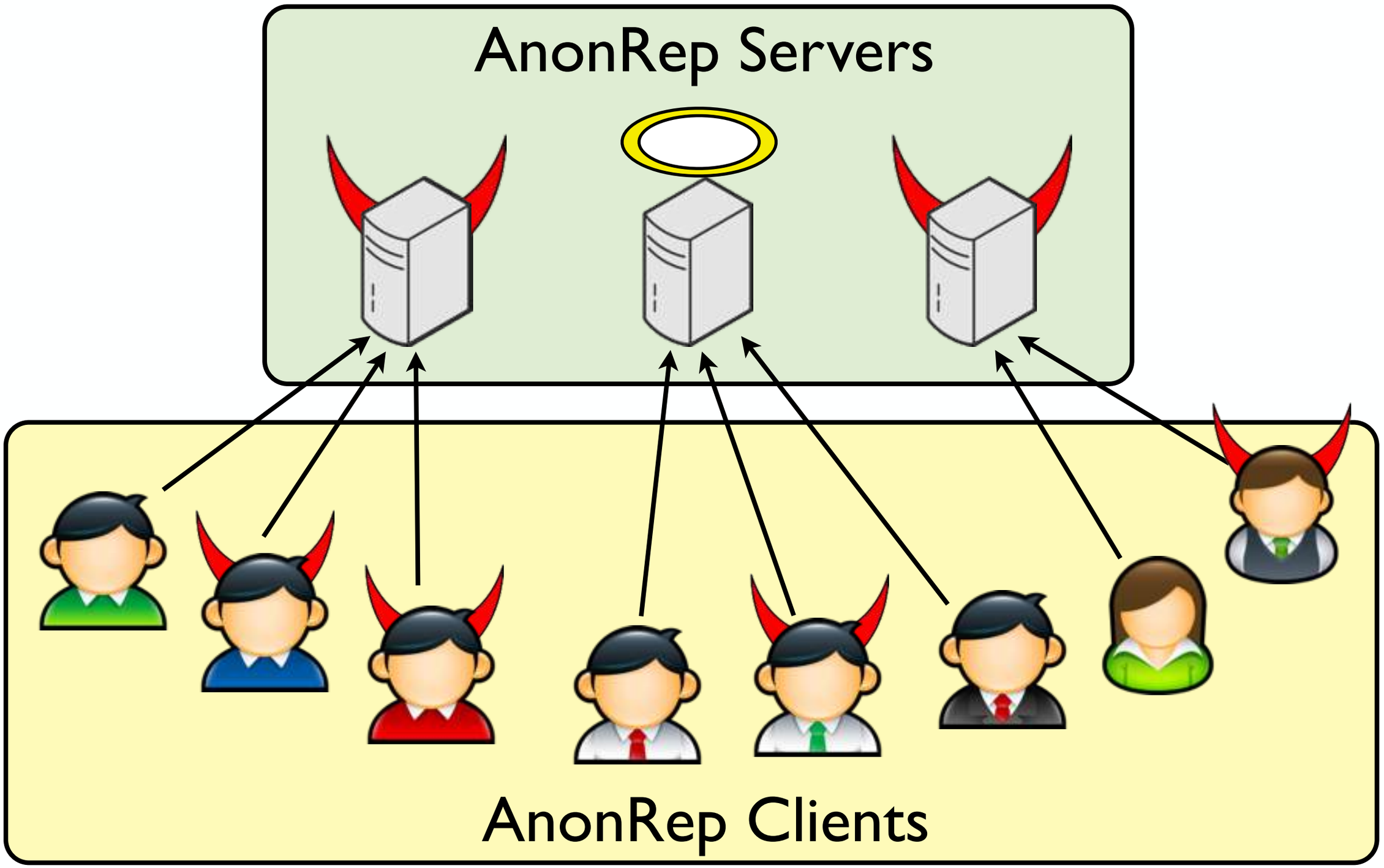
AnonRep Deployment



Threat Model

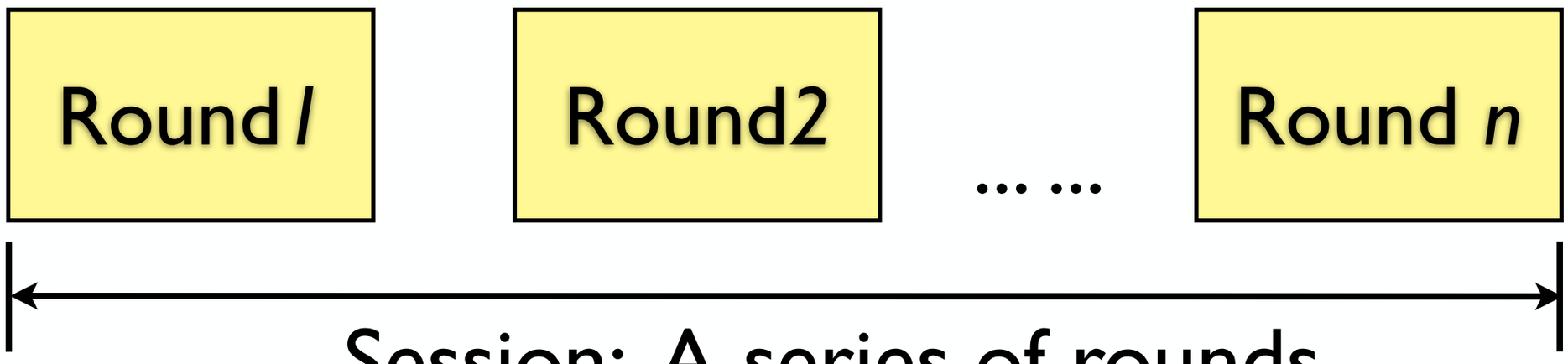


Threat Model



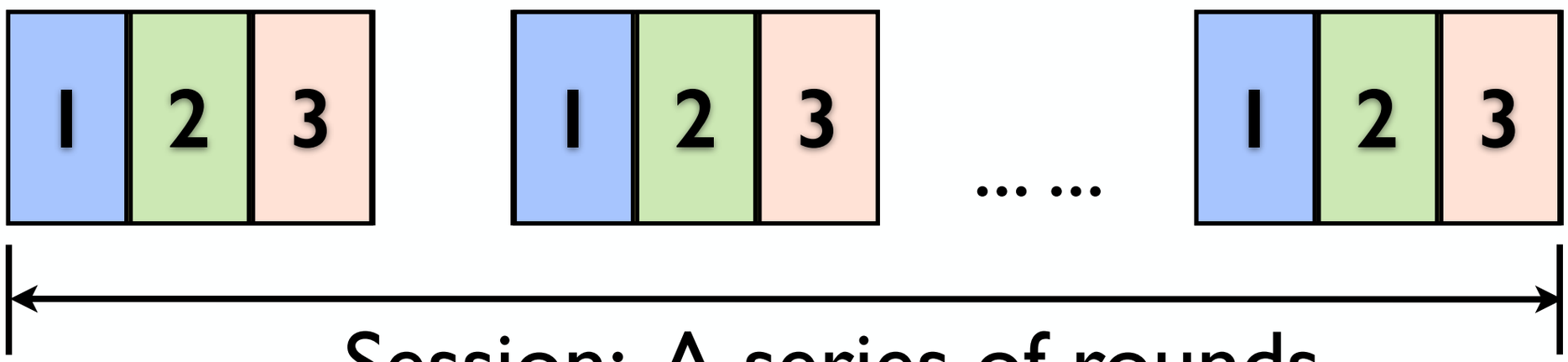
AnonRep Workflow

- Members (including servers and clients) participate in a continuous series of rounds



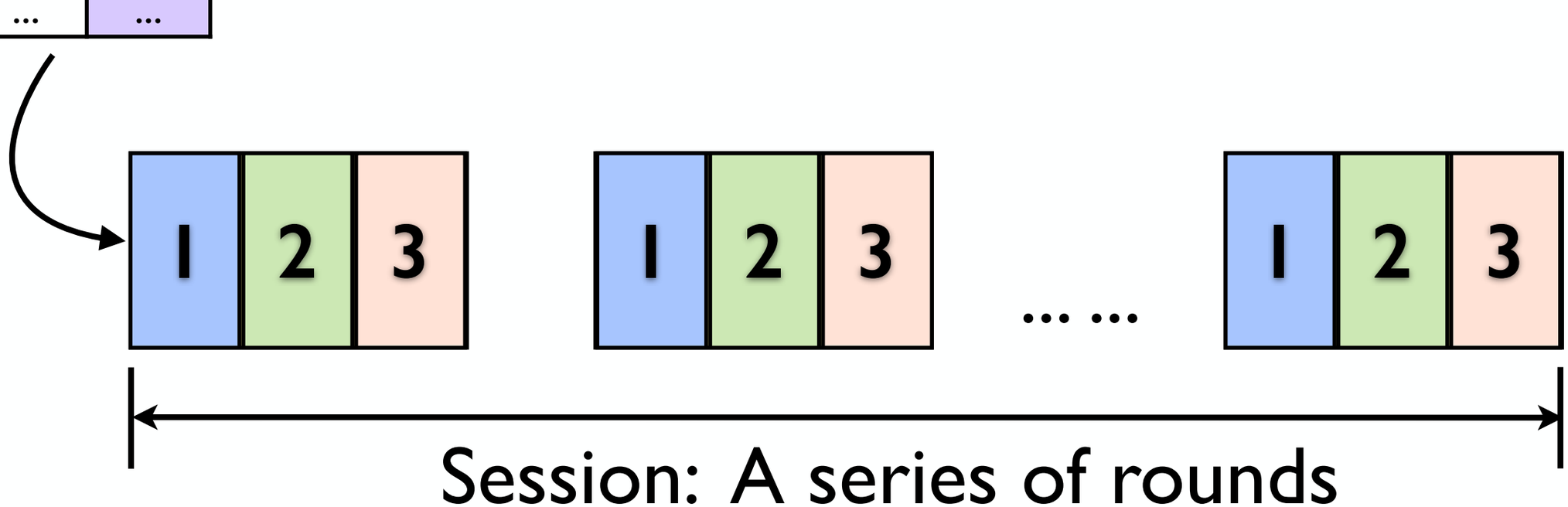
AnonRep Workflow

- Each round has three steps
  - Step1: Announcement
  - Step2: Message postings
  - Step3: Feedback collection

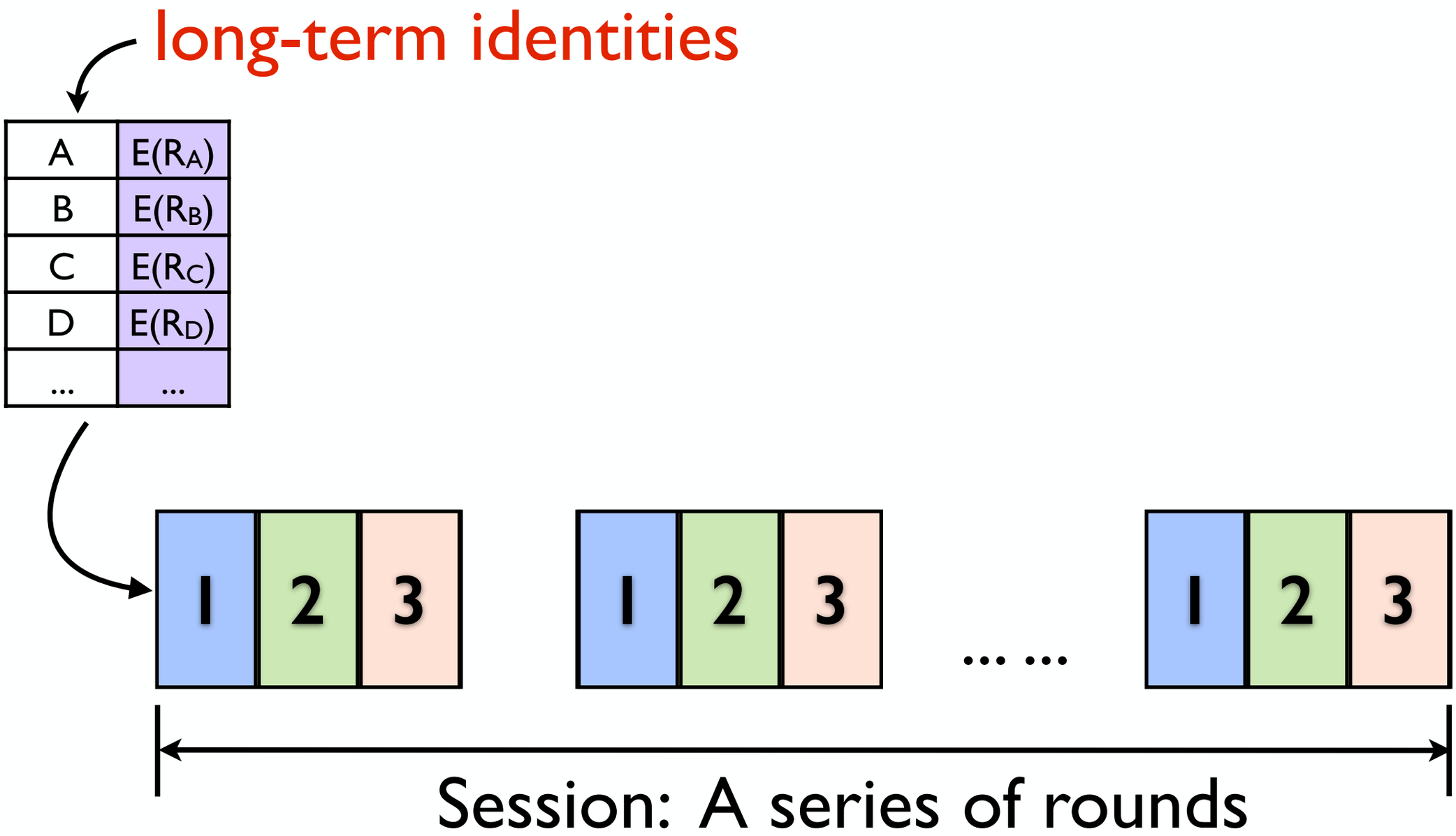


AnonRep Workflow

A	$E(R_A)$
B	$E(R_B)$
C	$E(R_C)$
D	$E(R_D)$
...	...



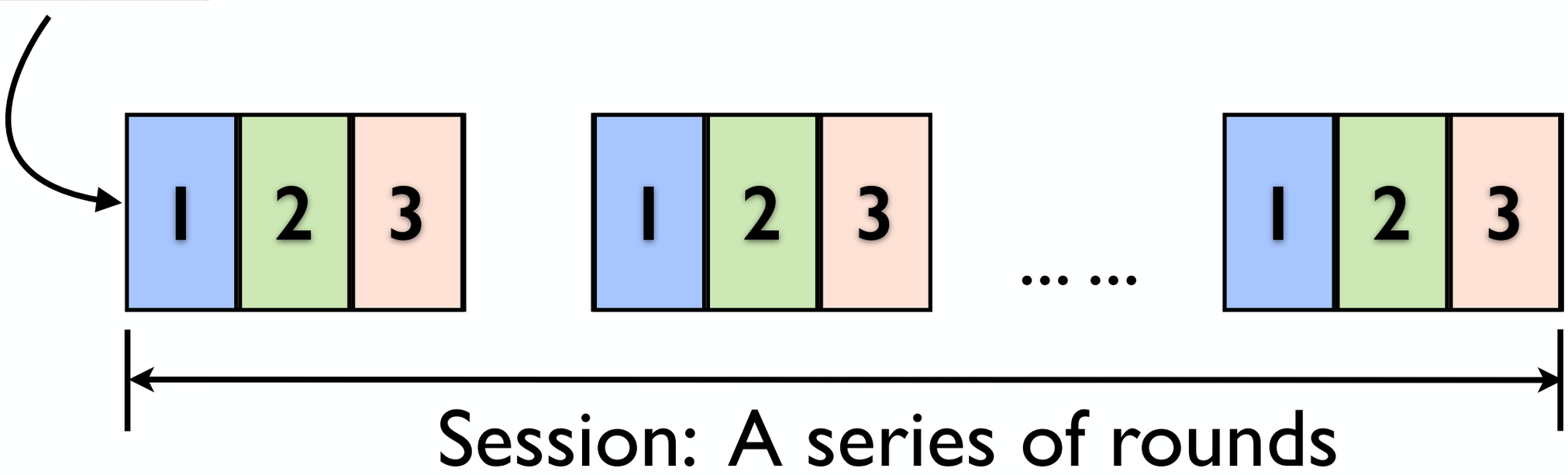
AnonRep Workflow



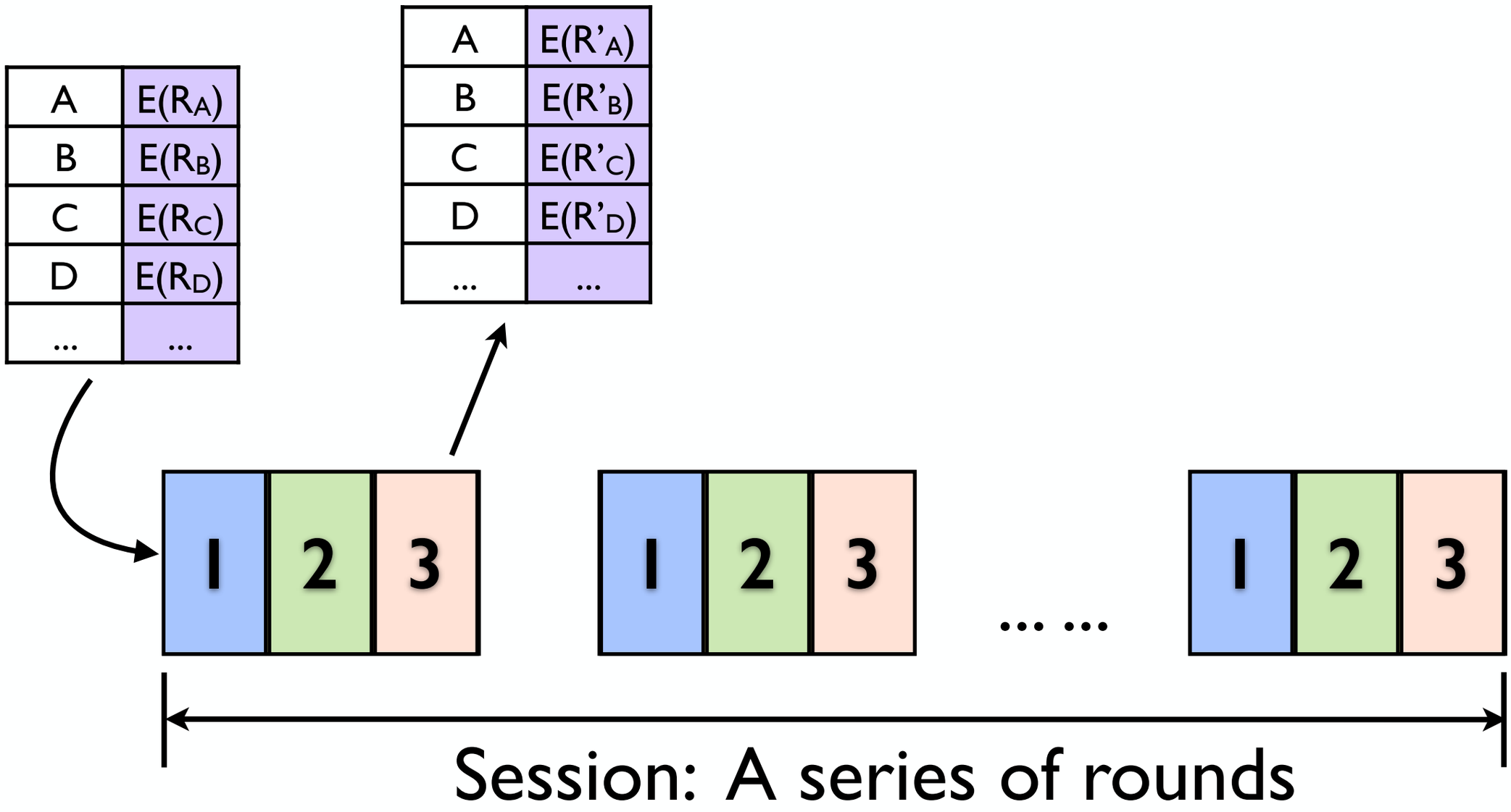
AnonRep Workflow

Reputation ciphertexts,
encrypted by all the servers

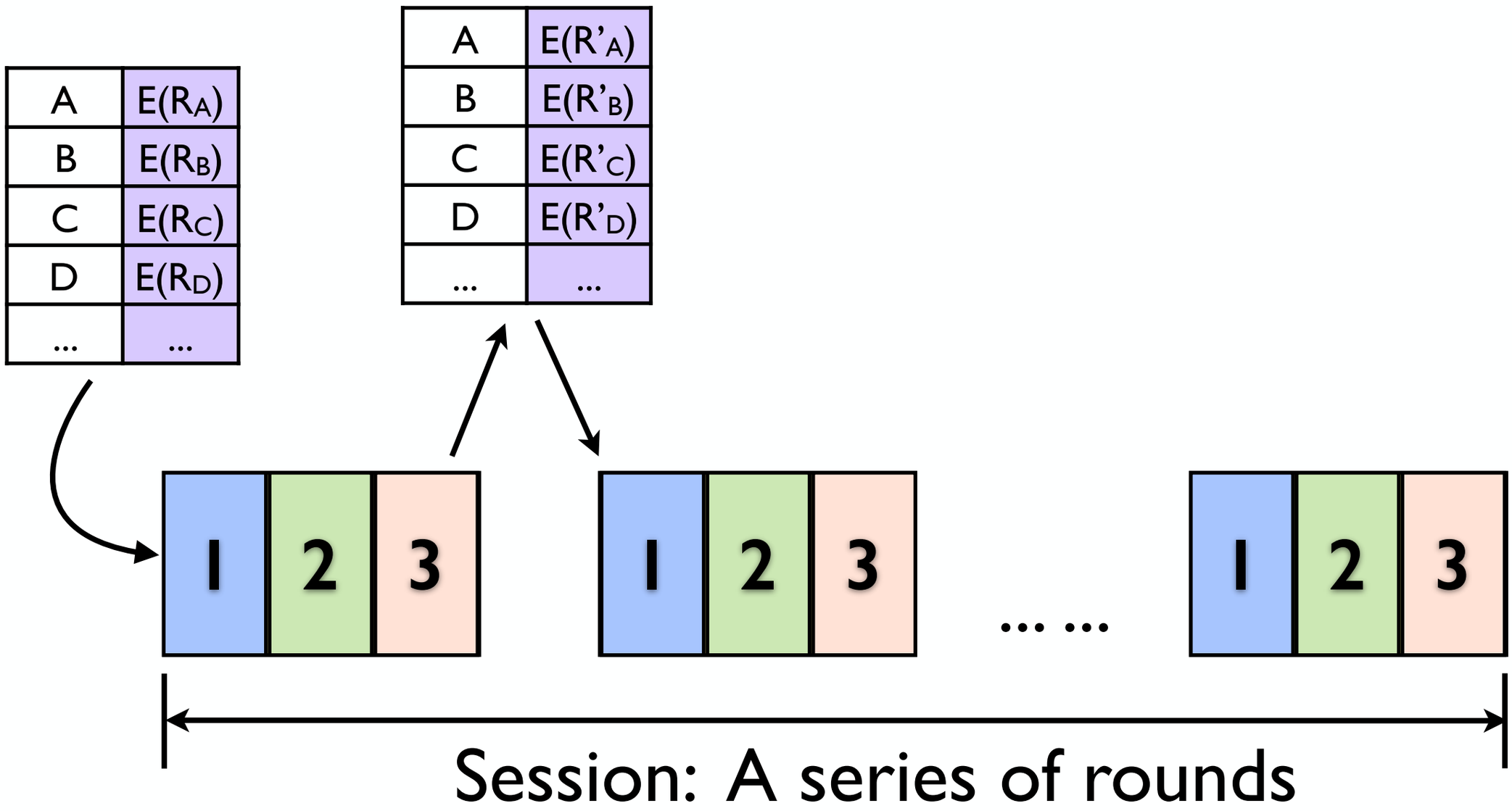
A	$E(R_A)$
B	$E(R_B)$
C	$E(R_C)$
D	$E(R_D)$
...	...



AnonRep Workflow



AnonRep Workflow



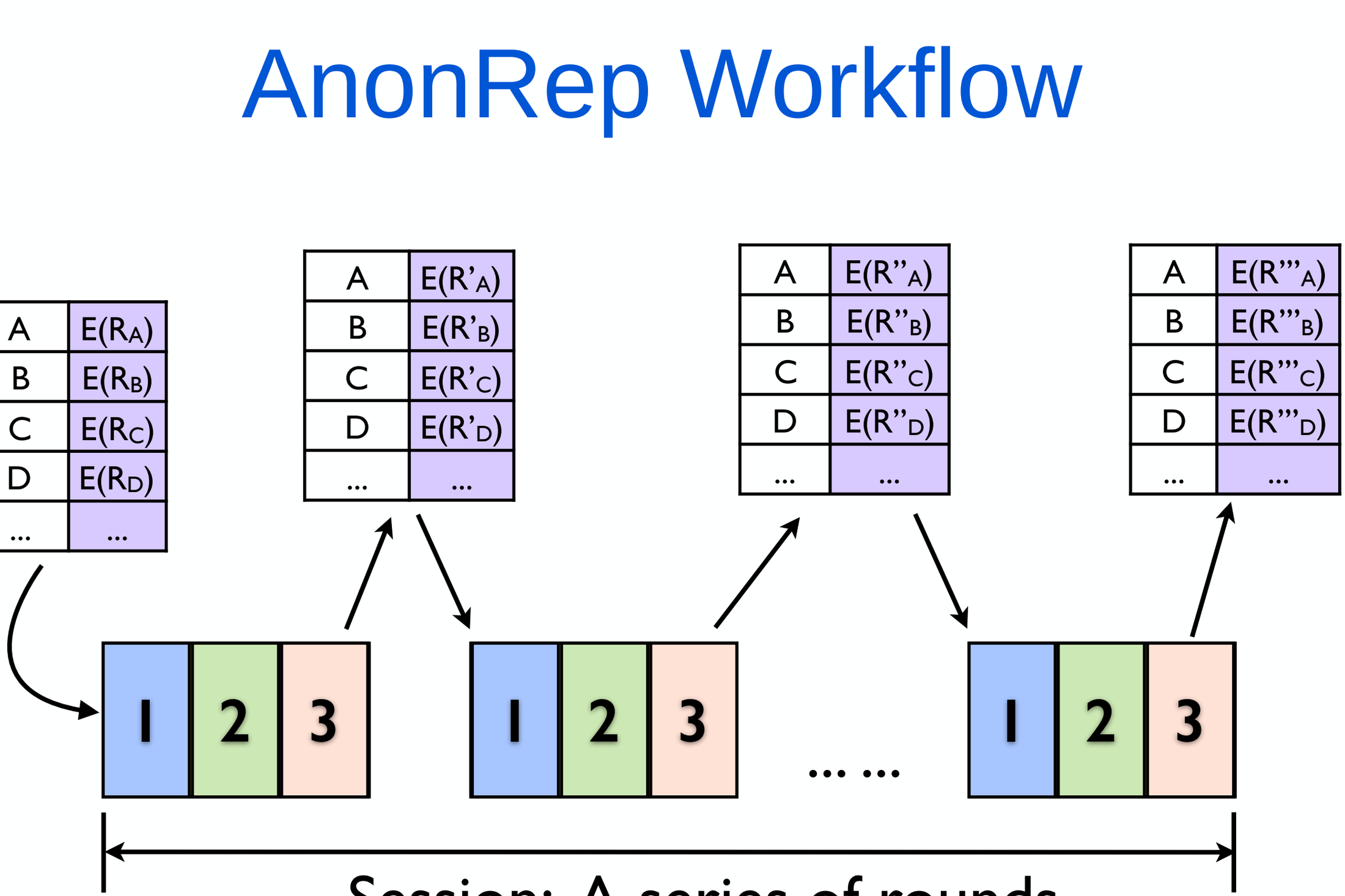
AnonRep Workflow

A	$E(R_A)$
B	$E(R_B)$
C	$E(R_C)$
D	$E(R_D)$
...	...

A	$E(R'_A)$
B	$E(R'_B)$
C	$E(R'_C)$
D	$E(R'_D)$
...	...

A	$E(R''_A)$
B	$E(R''_B)$
C	$E(R''_C)$
D	$E(R''_D)$
...	...

A	$E(R'''_A)$
B	$E(R'''_B)$
C	$E(R'''_C)$
D	$E(R'''_D)$
...	...



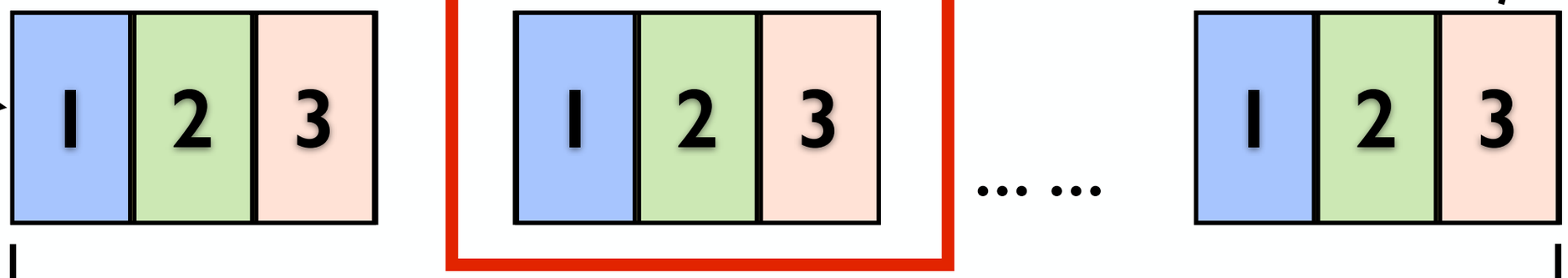
AnonRep Workflow

A	$E(R_A)$
B	$E(R_B)$
C	$E(R_C)$
D	$E(R_D)$
...	...

A	$E(R'_A)$
B	$E(R'_B)$
C	$E(R'_C)$
D	$E(R'_D)$
...	...

A	$E(R''_A)$
B	$E(R''_B)$
C	$E(R''_C)$
D	$E(R''_D)$
...	...

A	$E(R'''_A)$
B	$E(R'''_B)$
C	$E(R'''_C)$
D	$E(R'''_D)$
...	...



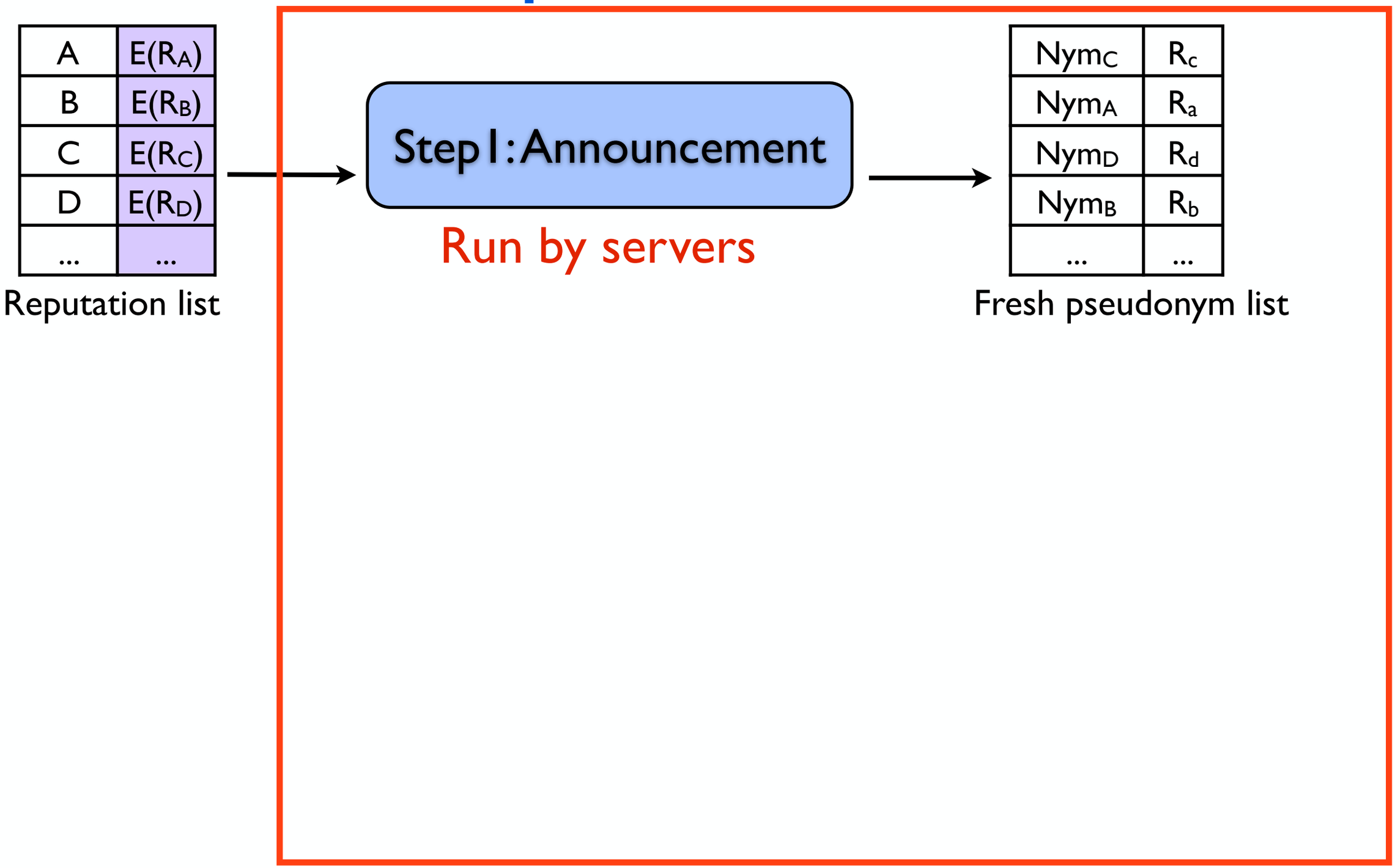
Session: A series of rounds

Three Steps in Each Round

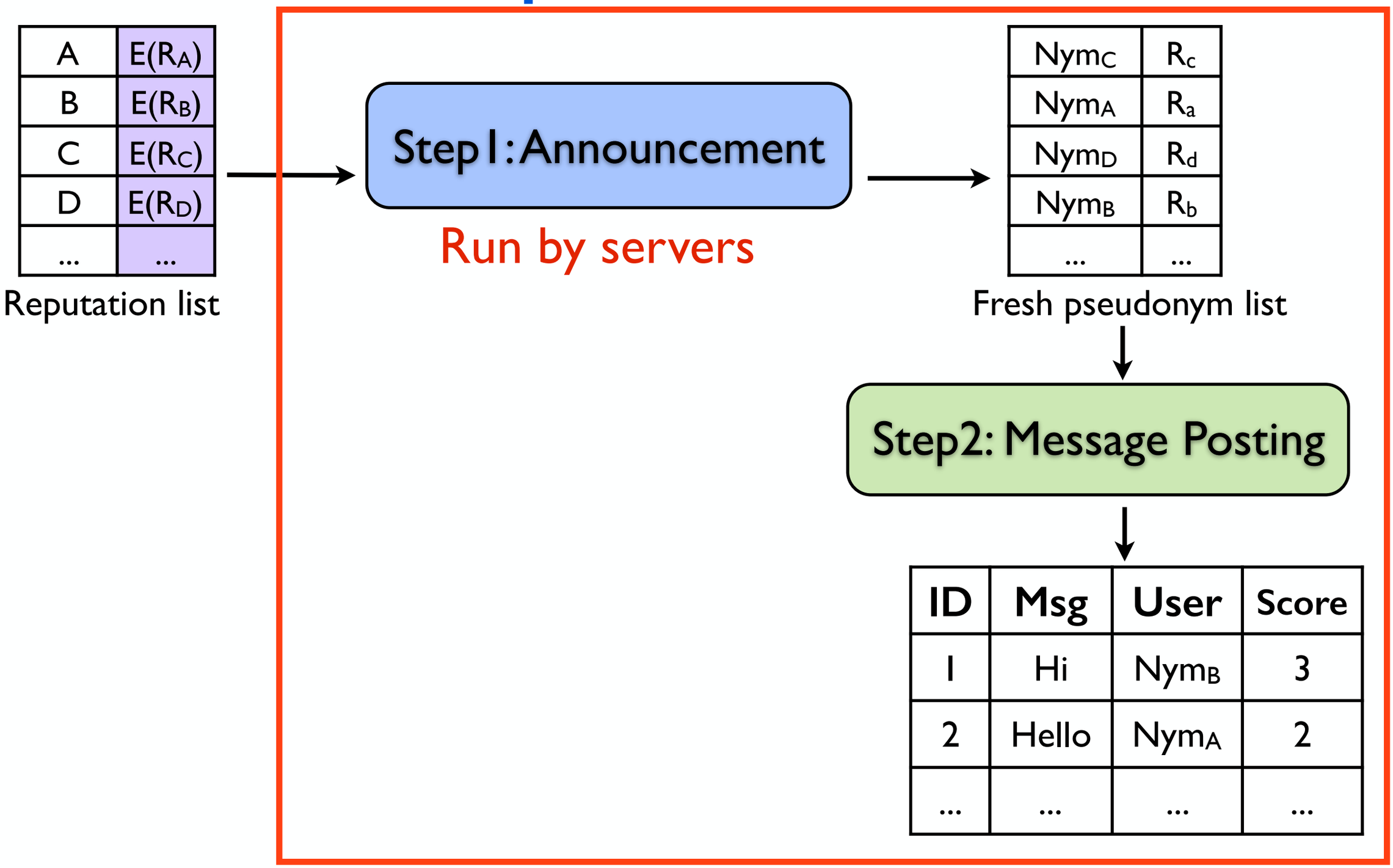
A	$E(R_A)$
B	$E(R_B)$
C	$E(R_C)$
D	$E(R_D)$
...	...

Reputation list

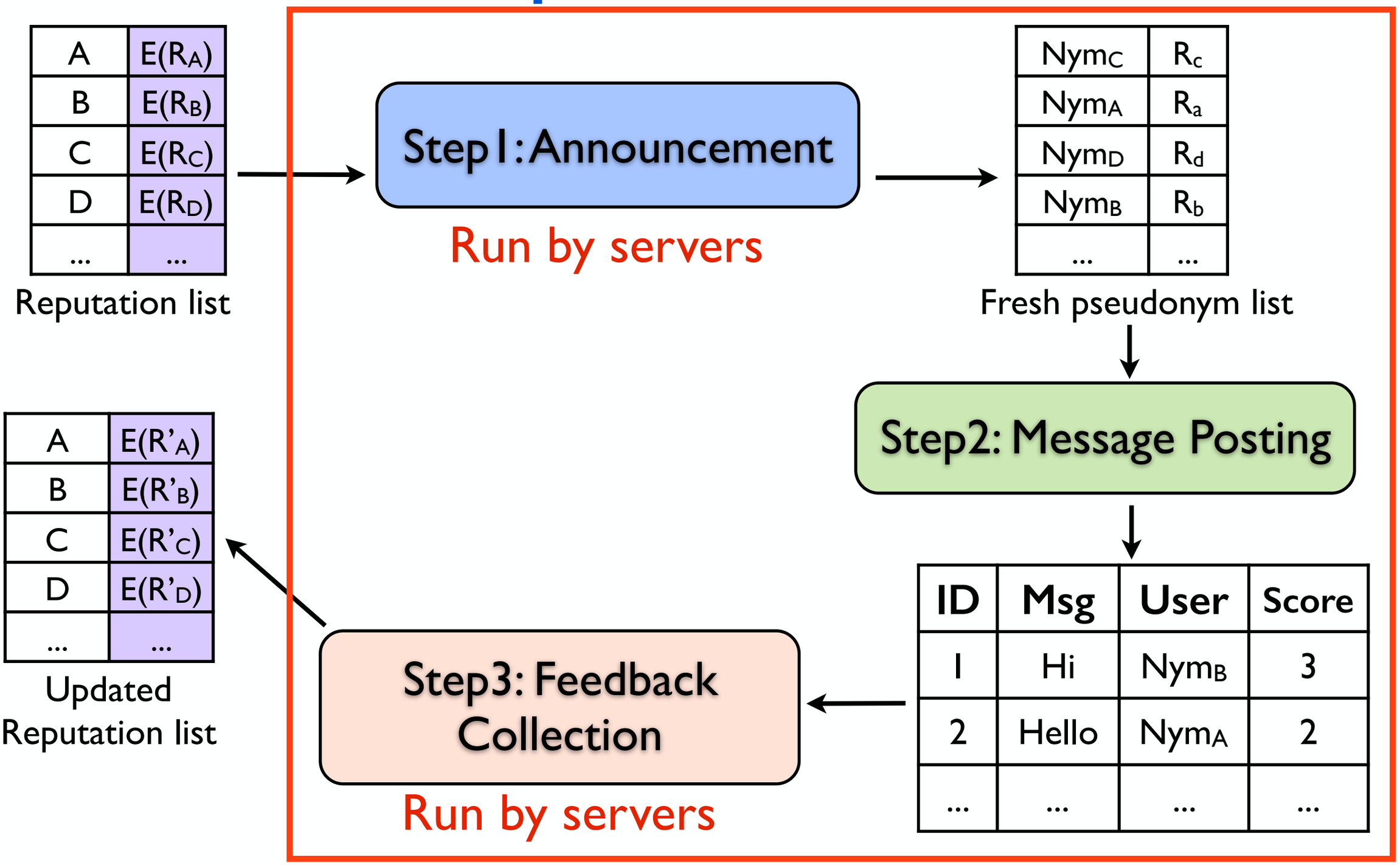
Three Steps in Each Round



Three Steps in Each Round

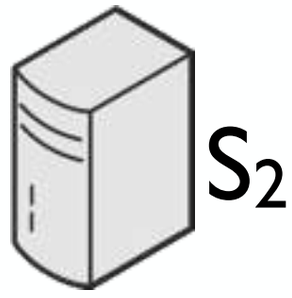


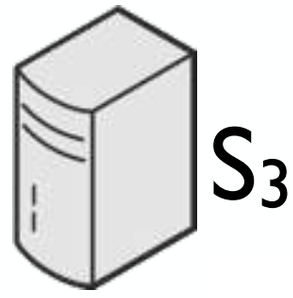
Three Steps in Each Round

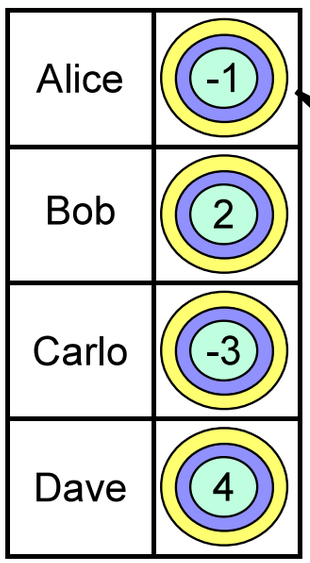


Step1: Announcement

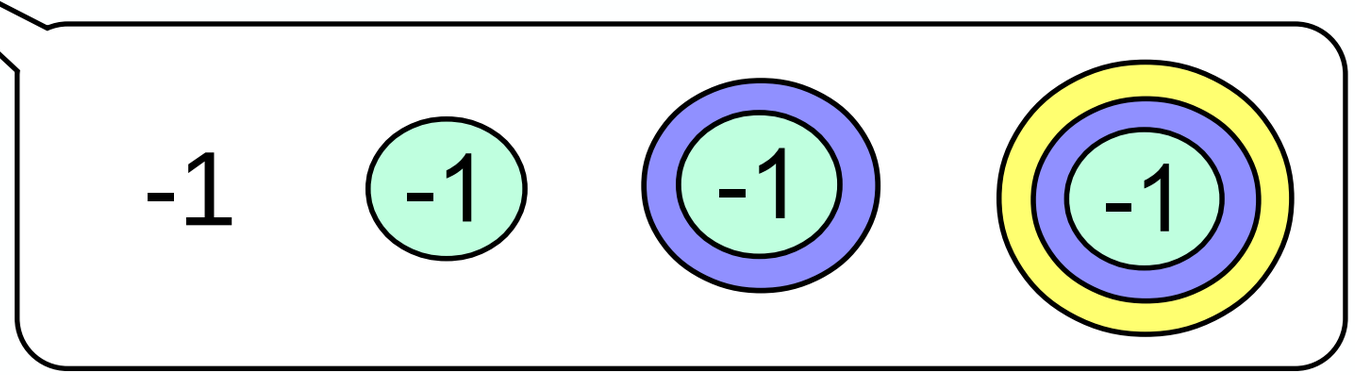
Step1: Announcement





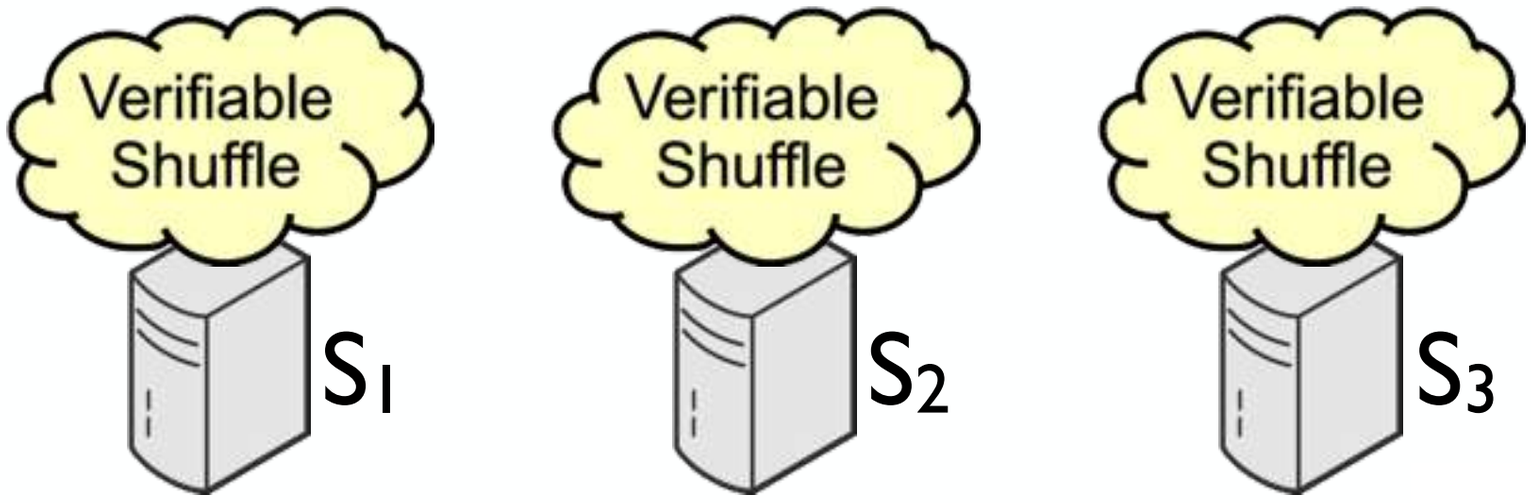


Reputation List



Reputations have been encrypted by all the servers

Step1: Announcement

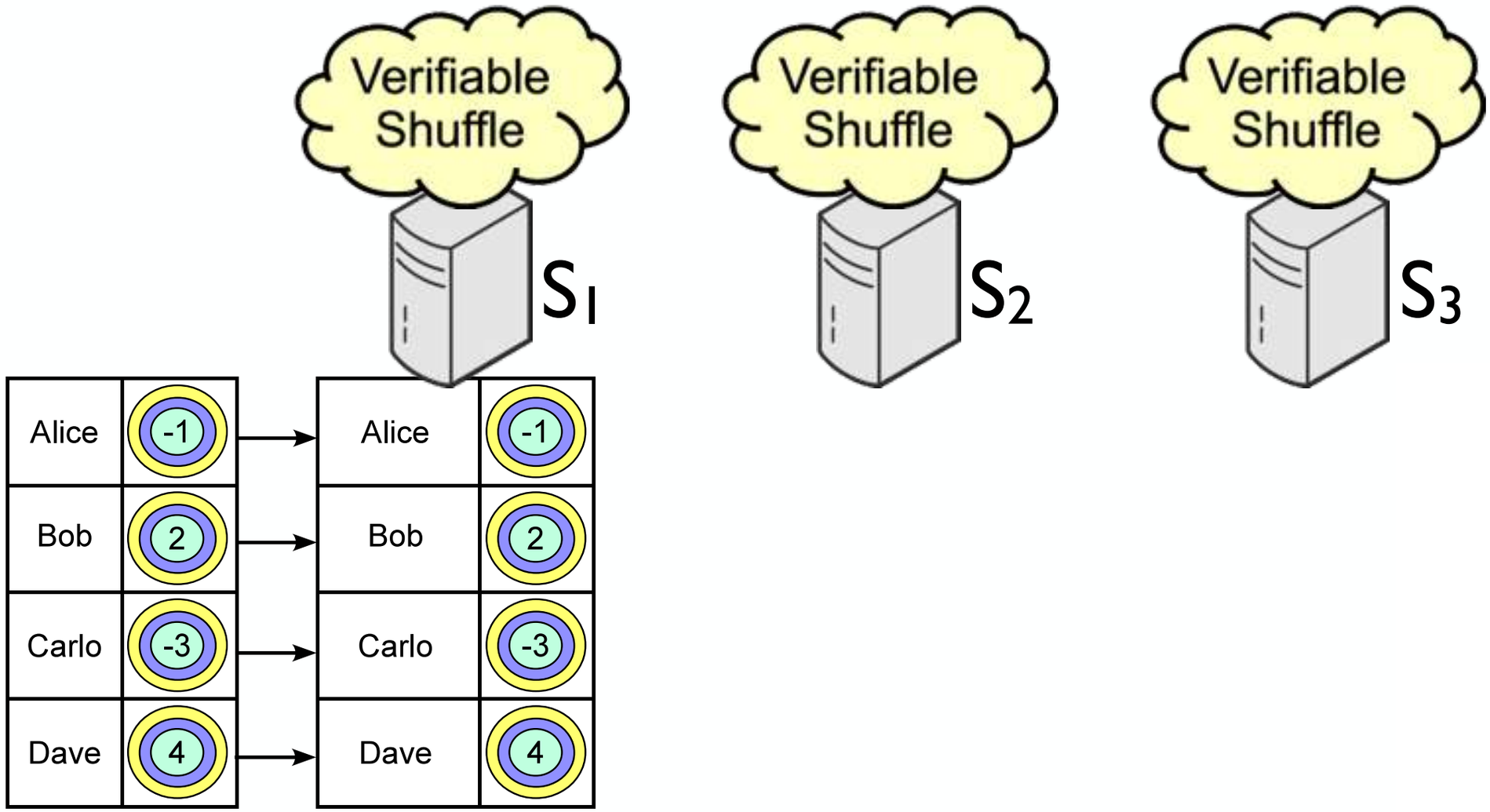


Alice	-1
Bob	2
Carlo	-3
Dave	4

Reputation List

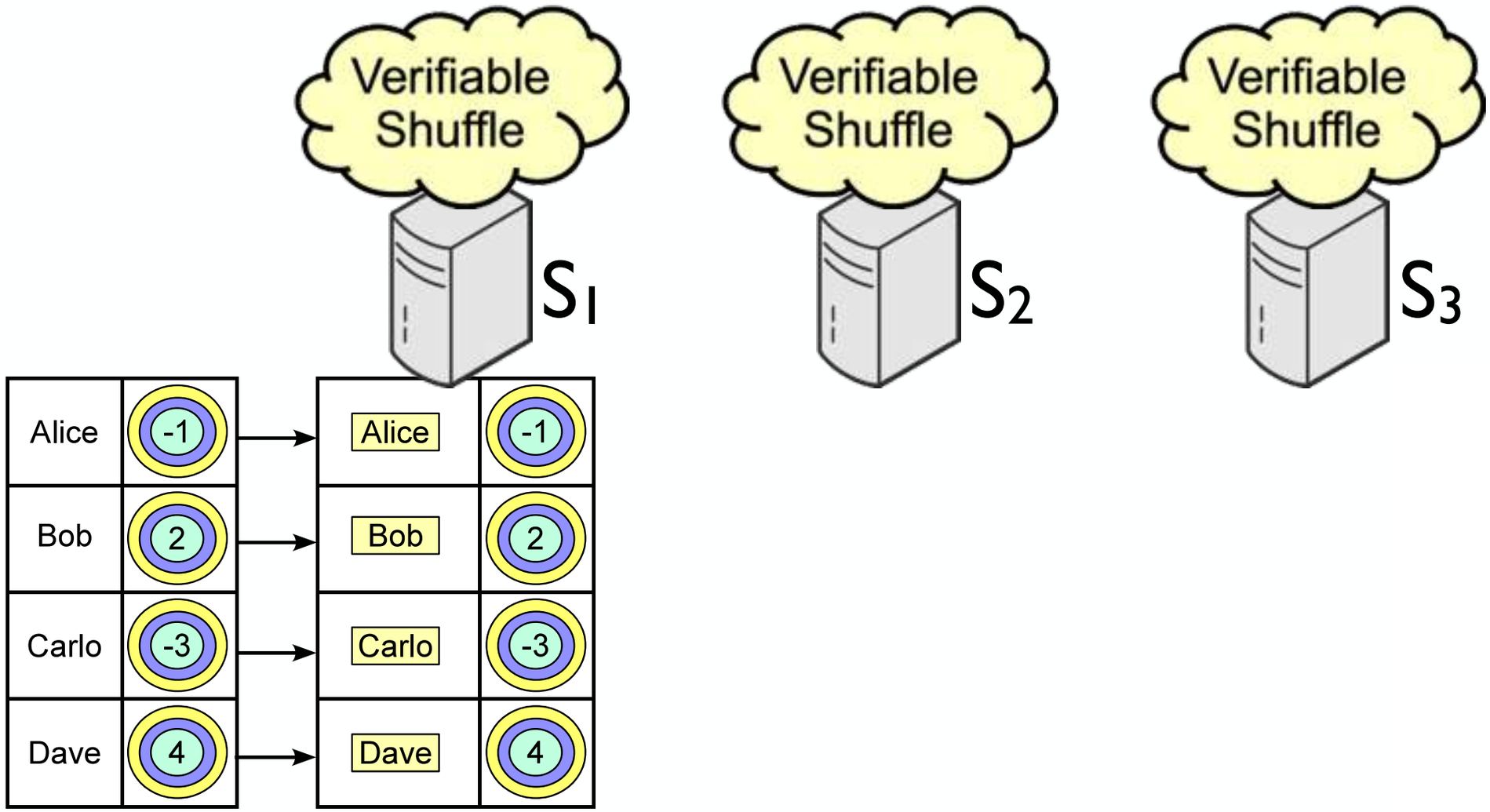
* C. Andrew Neff. A verifiable secret shuffle and its application to e-voting. In CCS'01.

Step1: Announcement



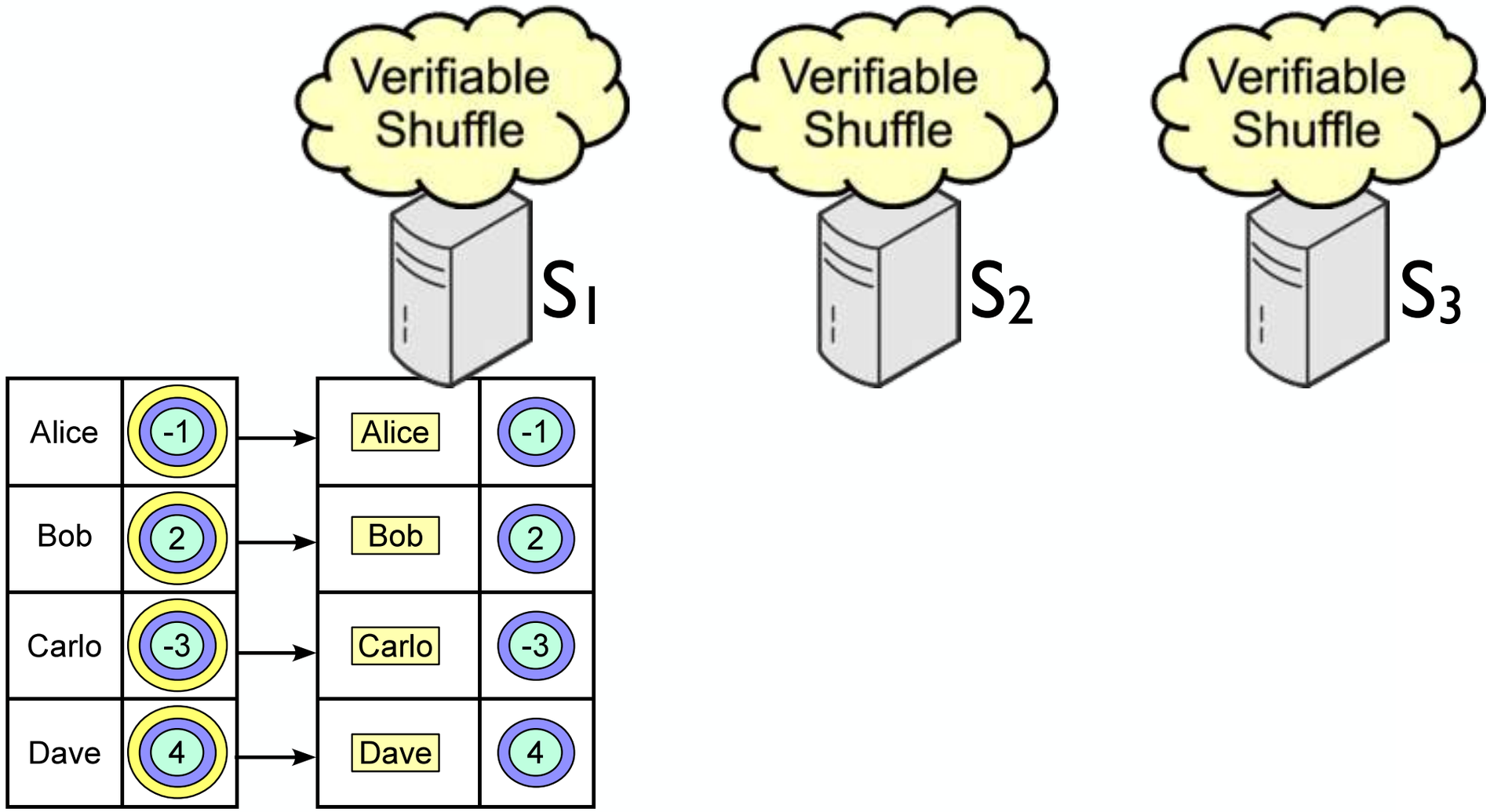
Reputation List

Step1: Announcement



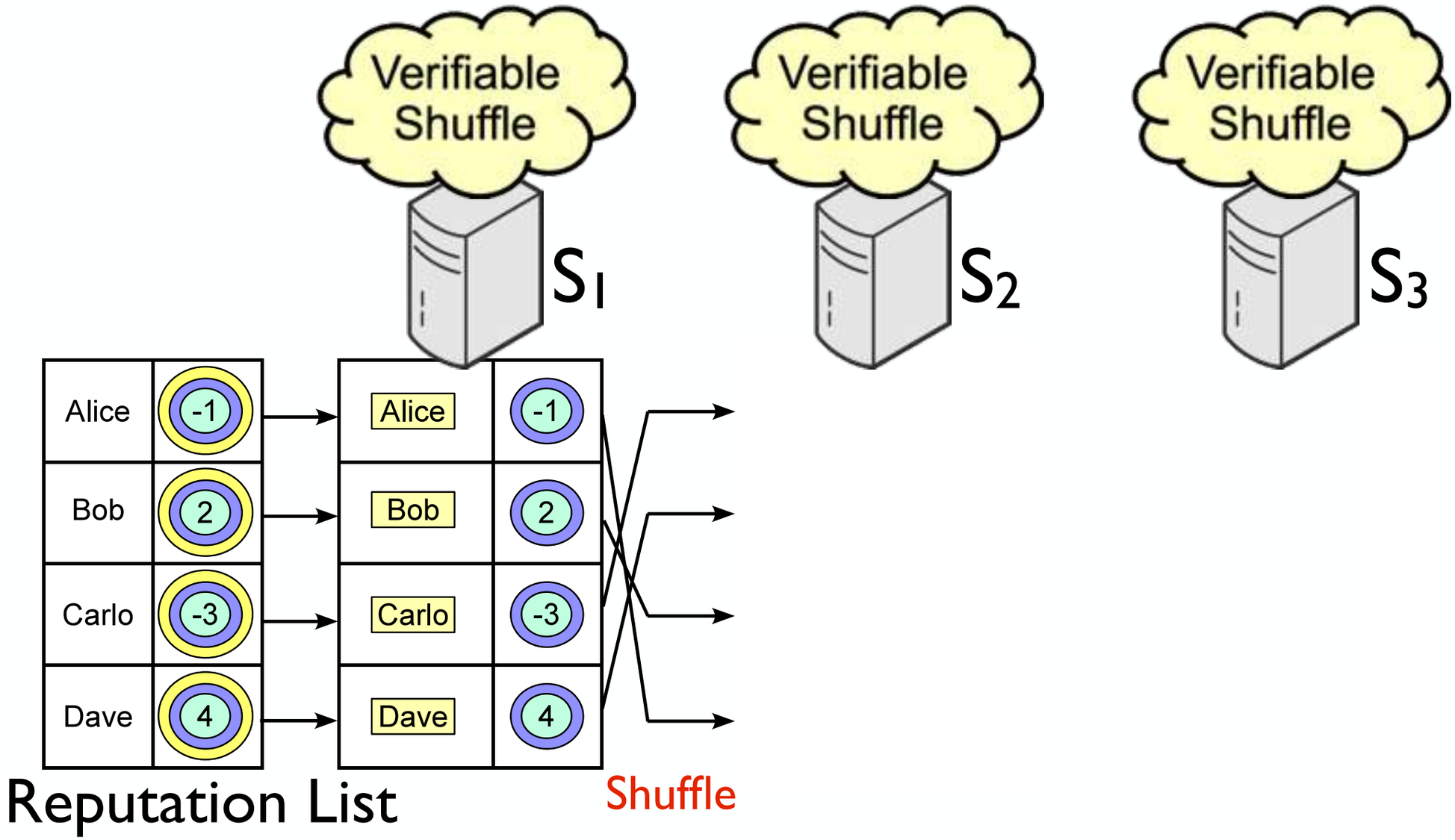
Reputation List

Step1: Announcement

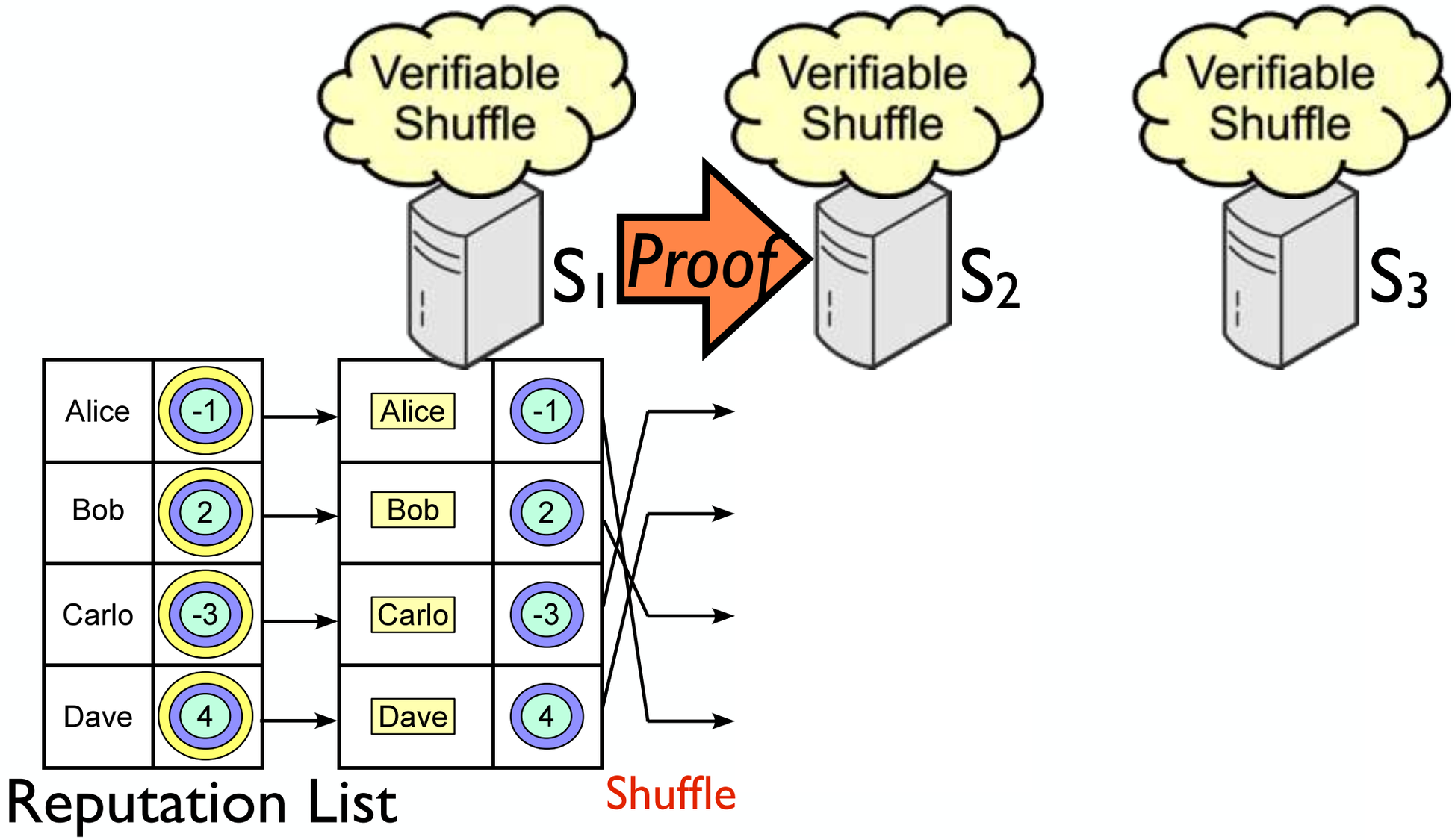


Reputation List

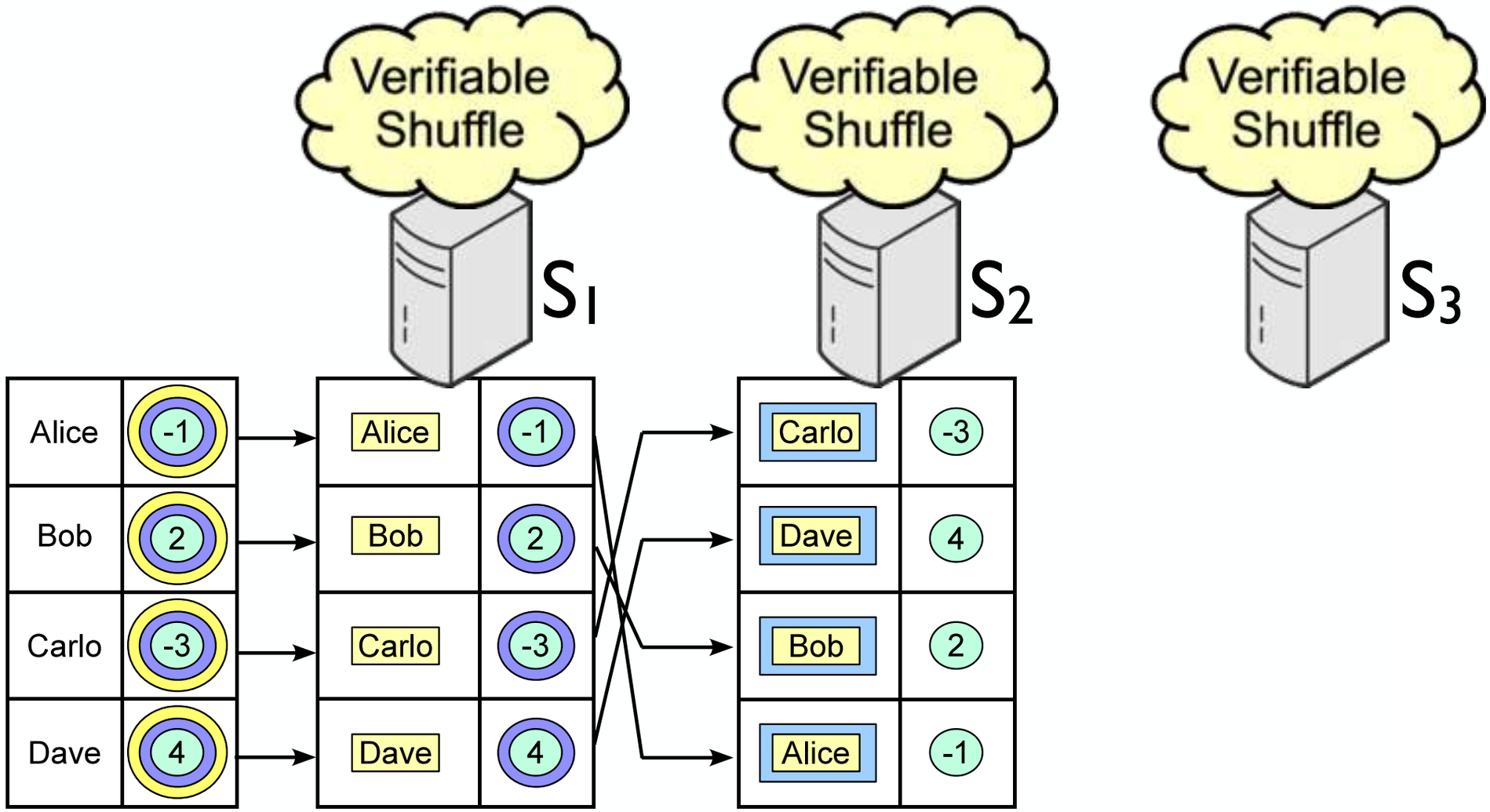
Step1: Announcement



Step1: Announcement

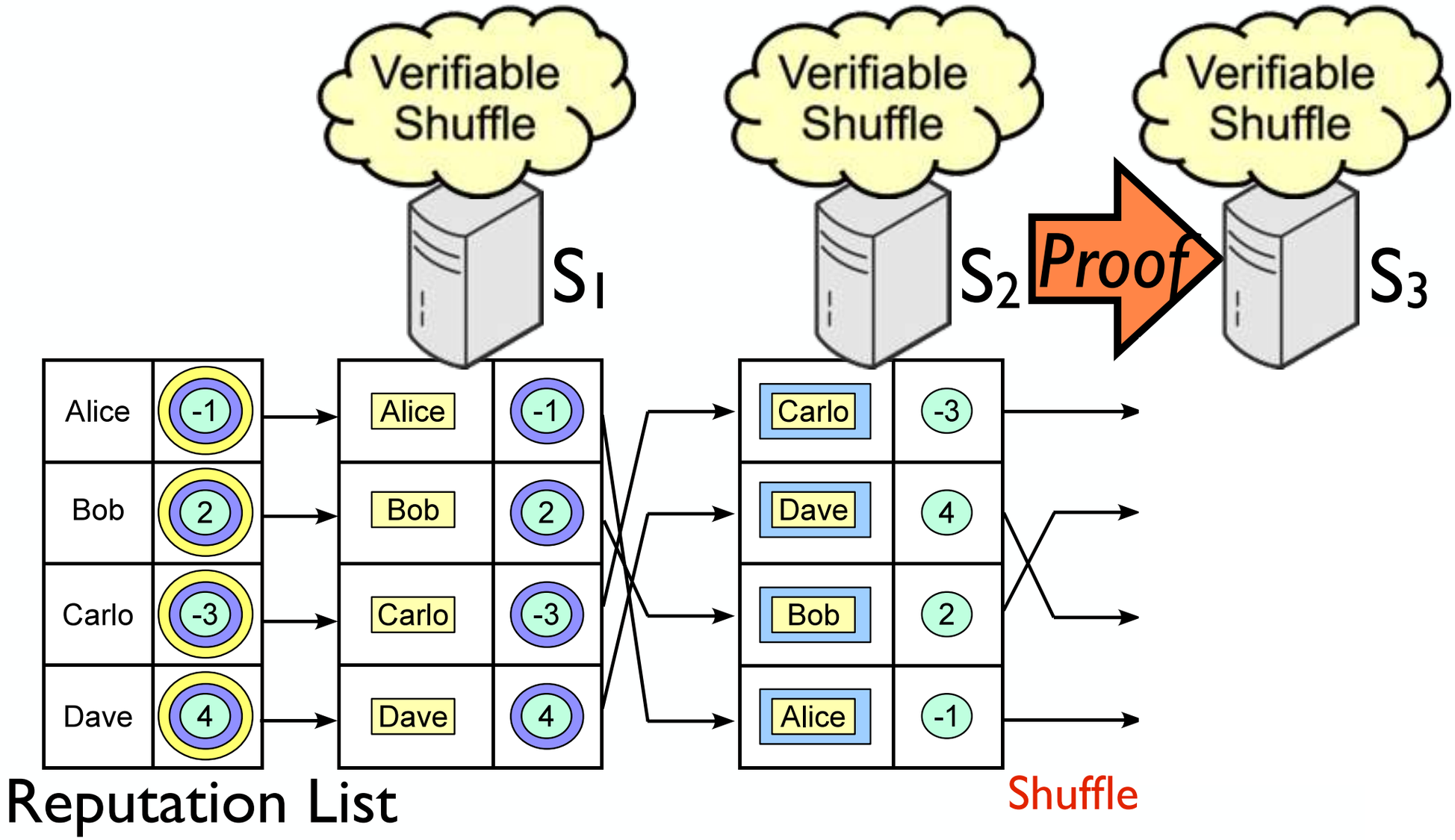


Step1: Announcement

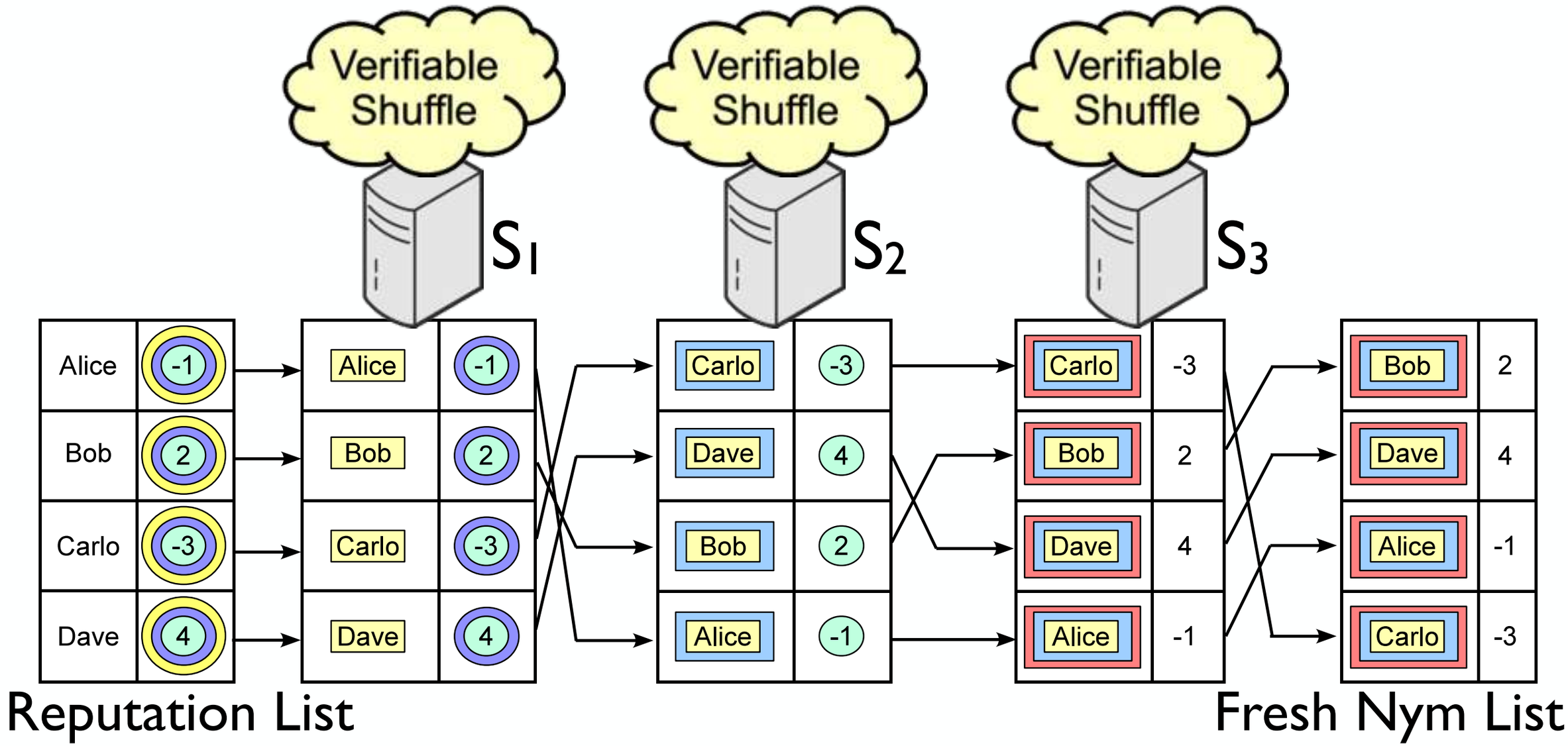


Reputation List

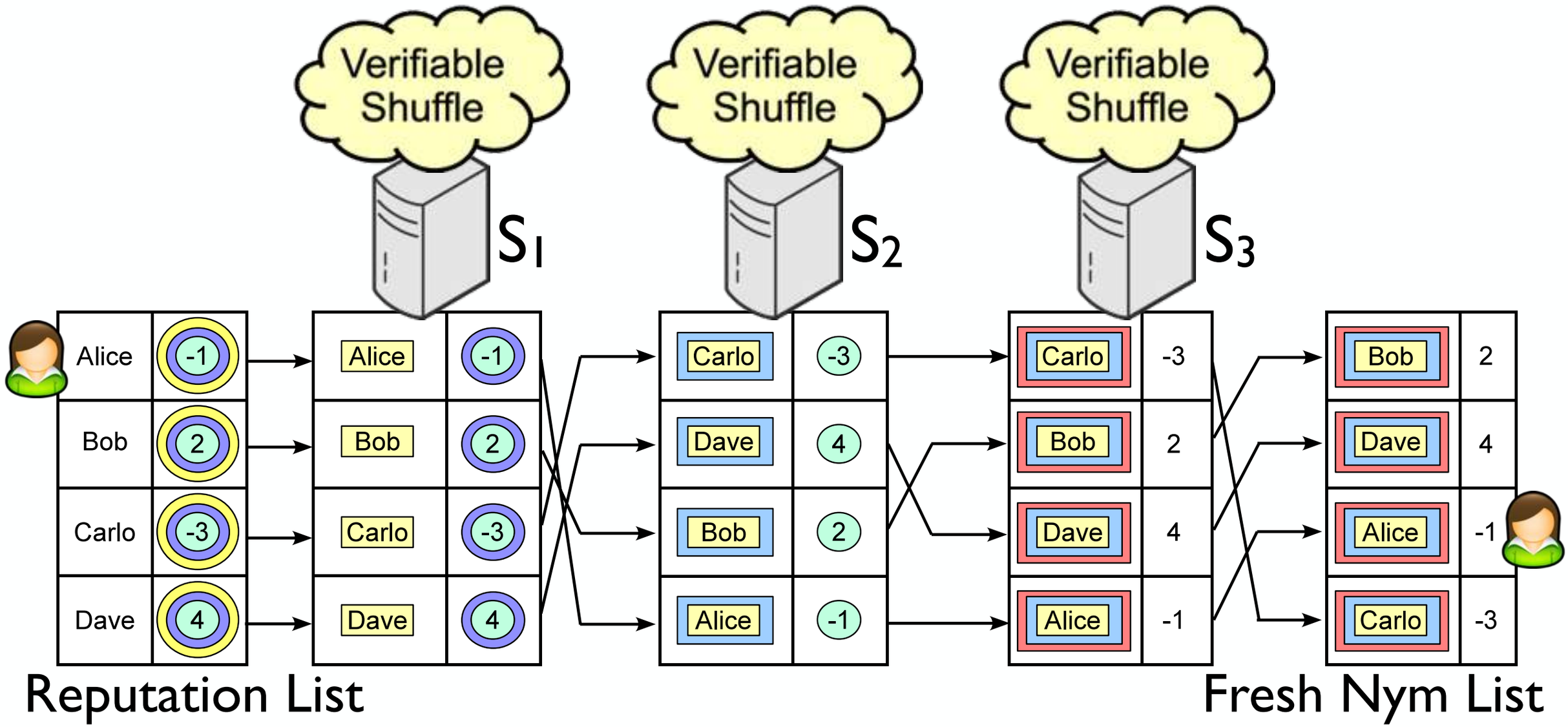
Step1: Announcement



Step1: Announcement



Step1: Announcement



Step2: Message Posting

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

Fresh Nym List

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

Fresh Nym List

MsgID	Msg	User	Score
...	...	...	...

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

Fresh Nym List

MsgID	Msg	User	Score
...	...	...	...

Bob

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

Fresh Nym List

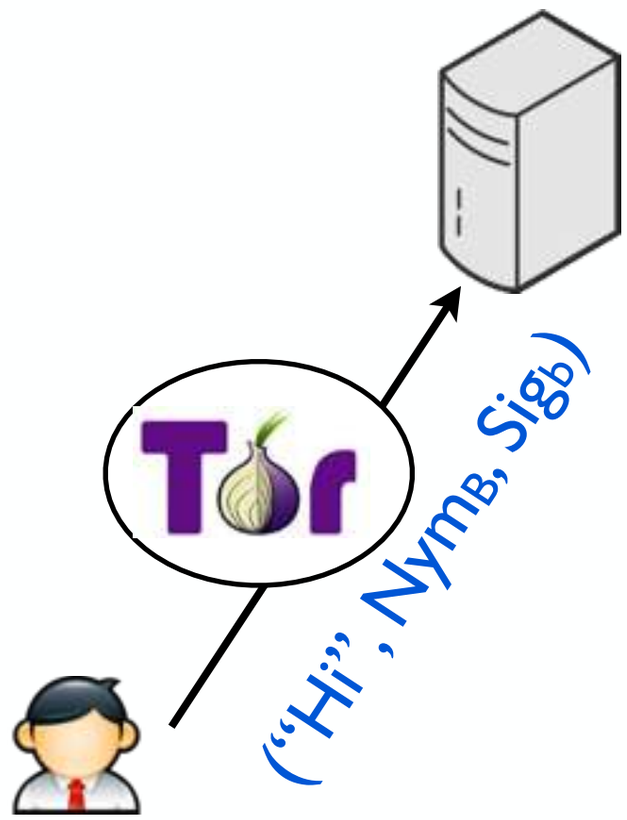
MsgID	Msg	User	Score
...	...	...	...

Bob ("Hi", Nym_B, Sig_b)

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

Fresh Nym List

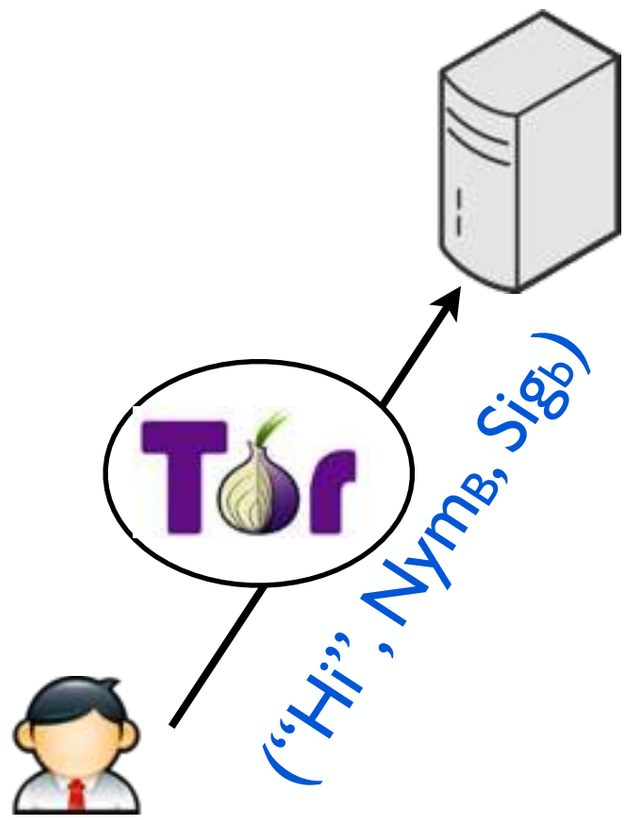


MsgID	Msg	User	Score
...	...	...	...

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

Fresh Nym List

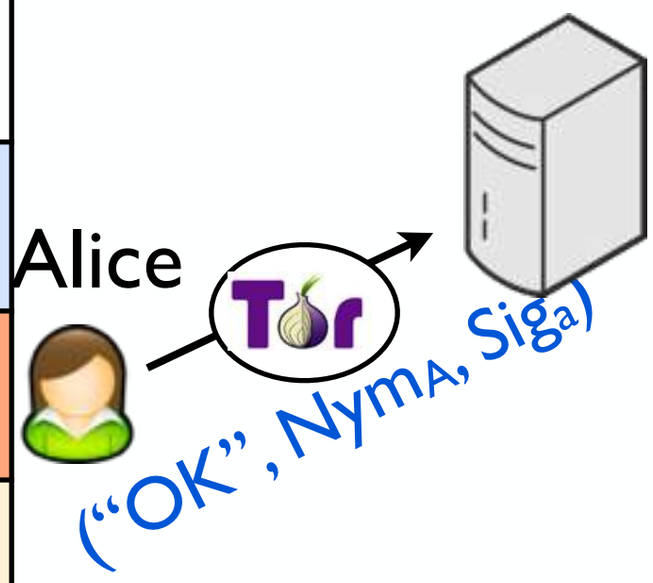


MsgID	Msg	User	Score
Msg1	Hi	Nym_B	3
...	...	...	...

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

Fresh Nym List

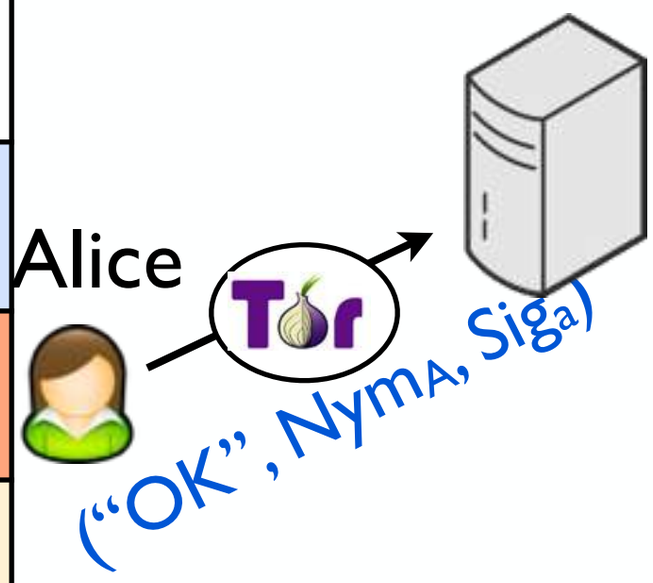


MsgID	Msg	User	Score
Msg1	Hi	Nym_B	3
...	...	...	...

Step2: Message Posting

Nym	Score
Nym_C	-2
Nym_A	2
Nym_D	-1
Nym_B	3
...	...

Fresh Nym List



MsgID	Msg	User	Score
Msg1	Hi	Nym_B	3
Msg2	OK	Nym_A	2
...	...	...	...

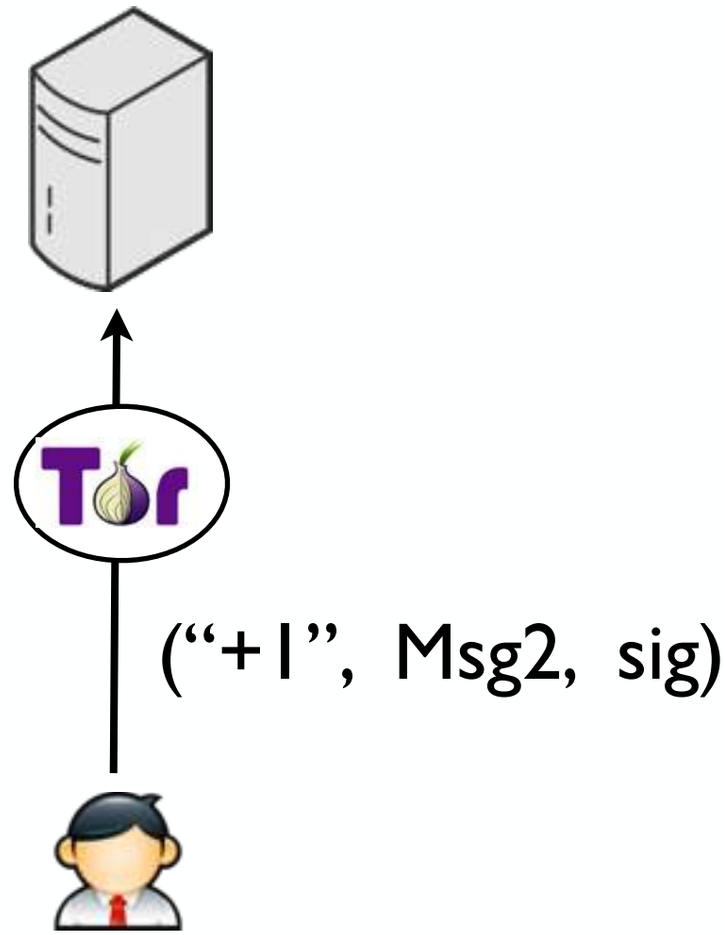
Step3: Feedback Collection

Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	
Msg2	Hello	Nym_A	2	
…	…	…	…	

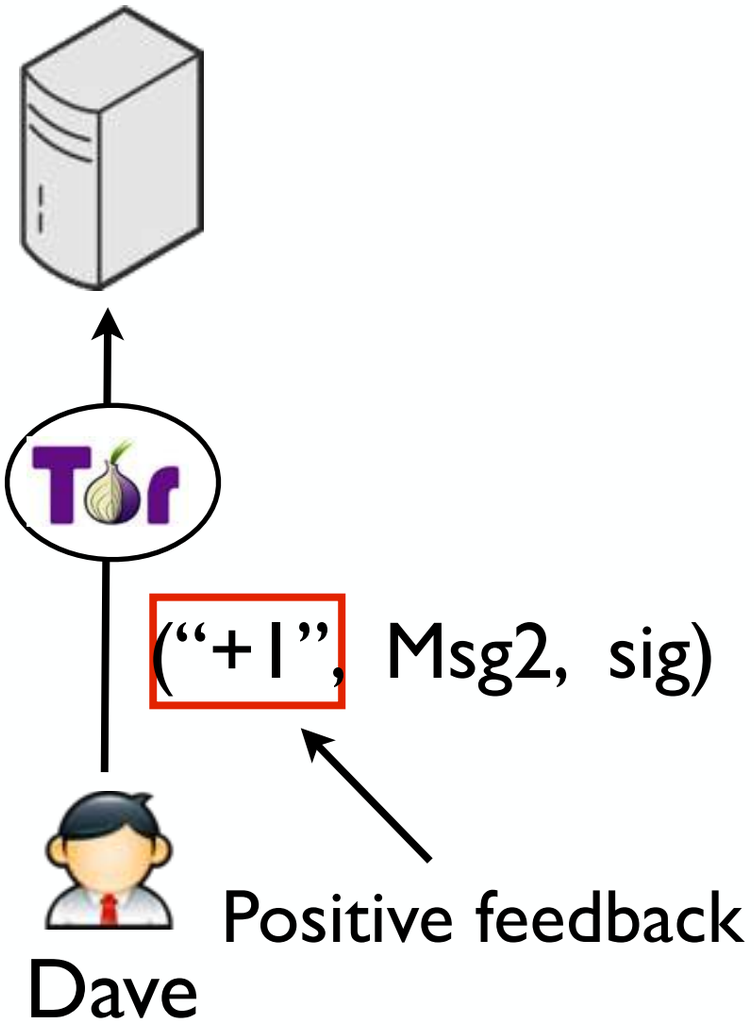
Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	
Msg2	Hello	Nym_A	2	
…	…	…	…	



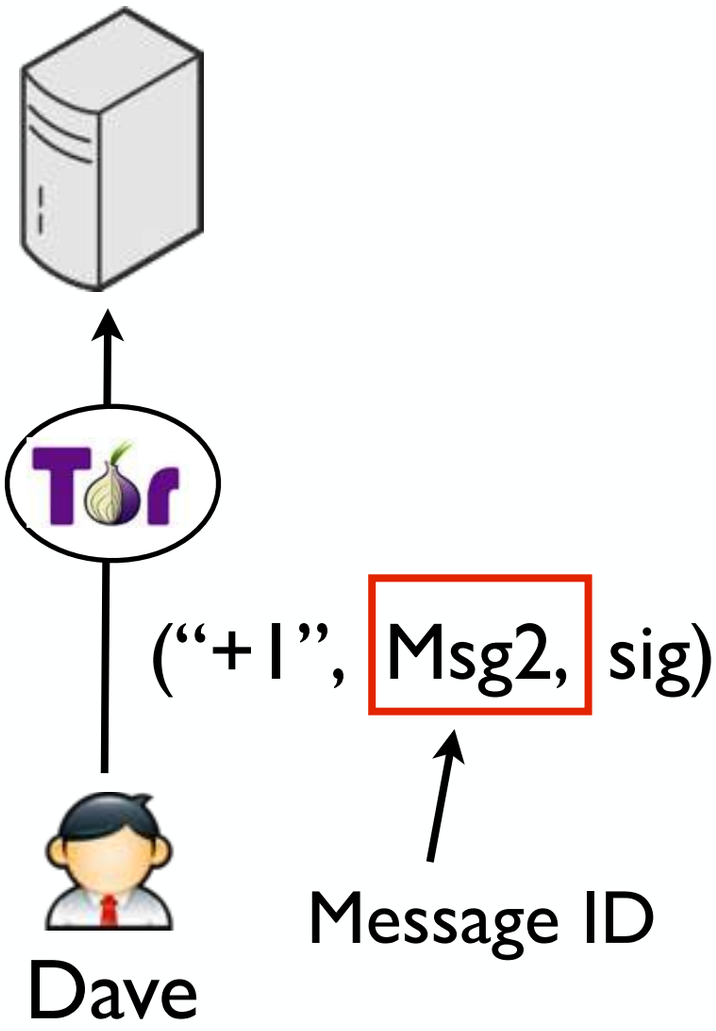
Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	
Msg2	Hello	Nym_A	2	
…	…	…	…	



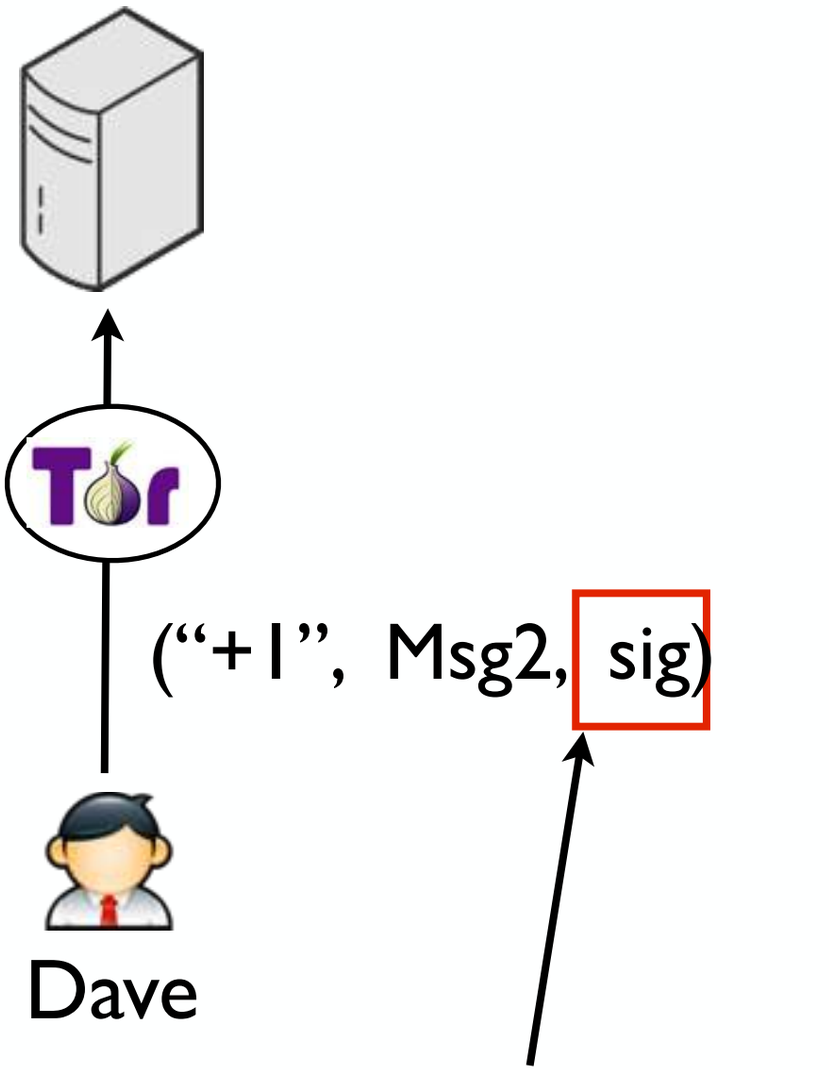
Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	
Msg2	Hello	Nym_A	2	
…	…	…	…	

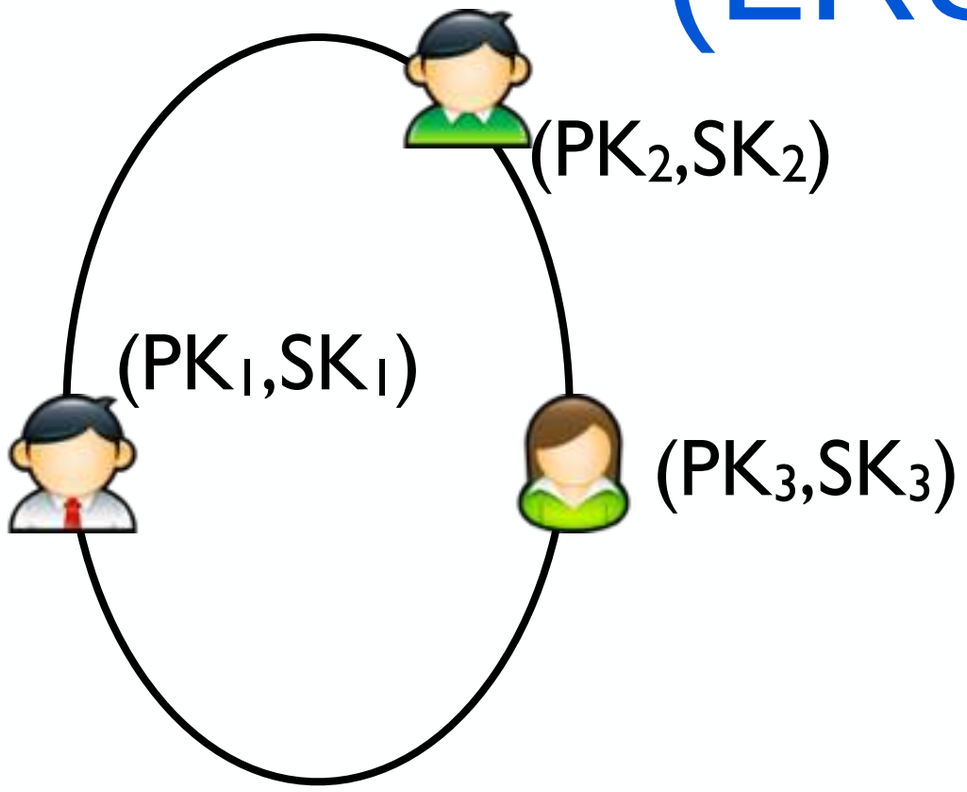


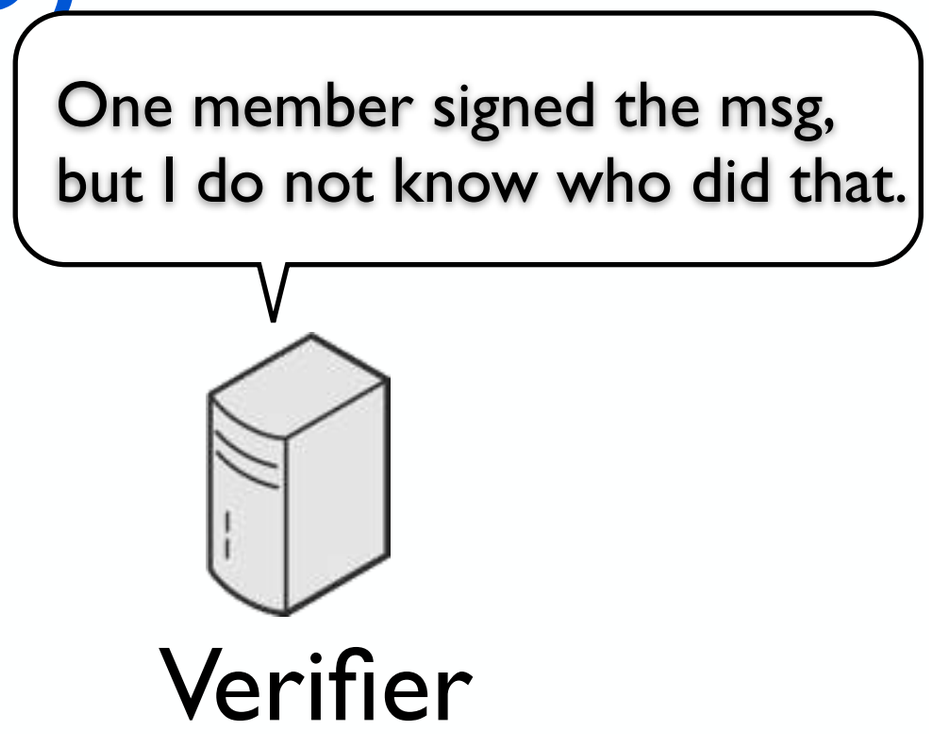
Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	
Msg2	Hello	Nym_A	2	
…	…	…	…	



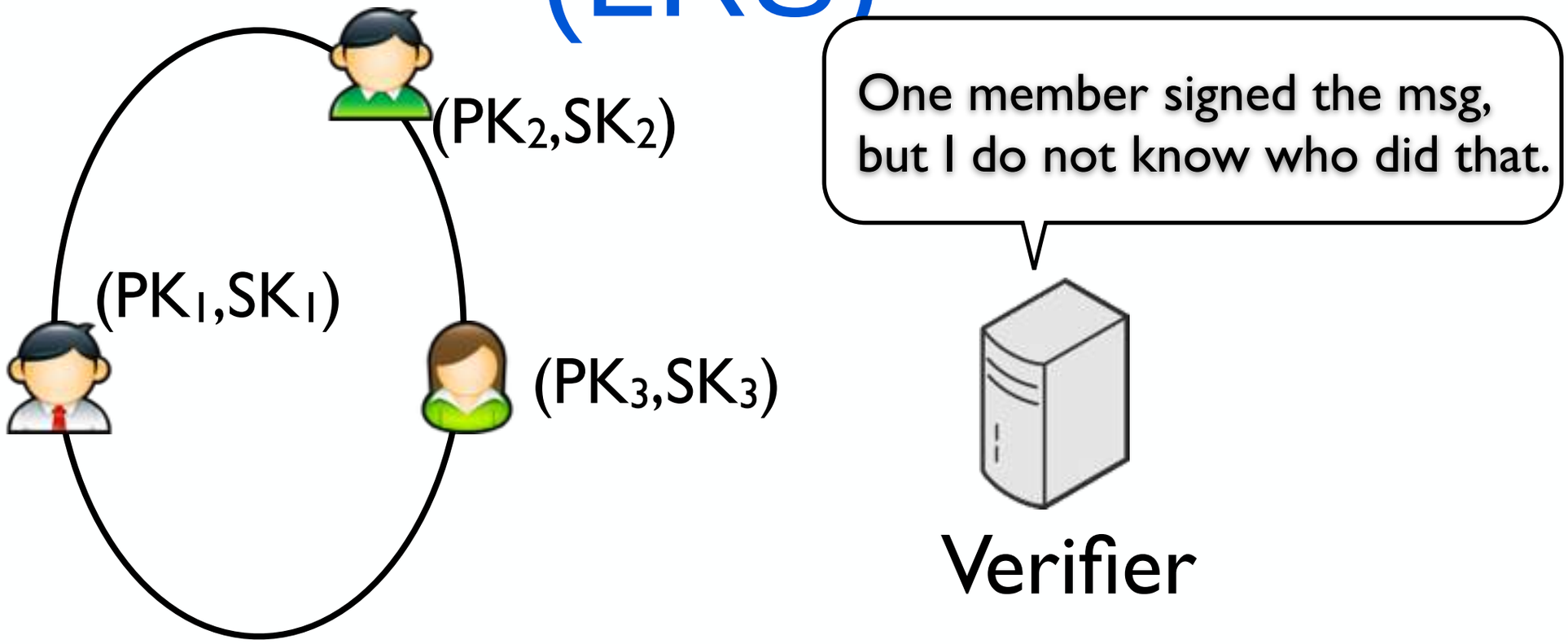
Linkable Ring Signature (LRS)





* Liu et al. Linkable ring signatures: Security models and new schemes. In ICCSA'05.

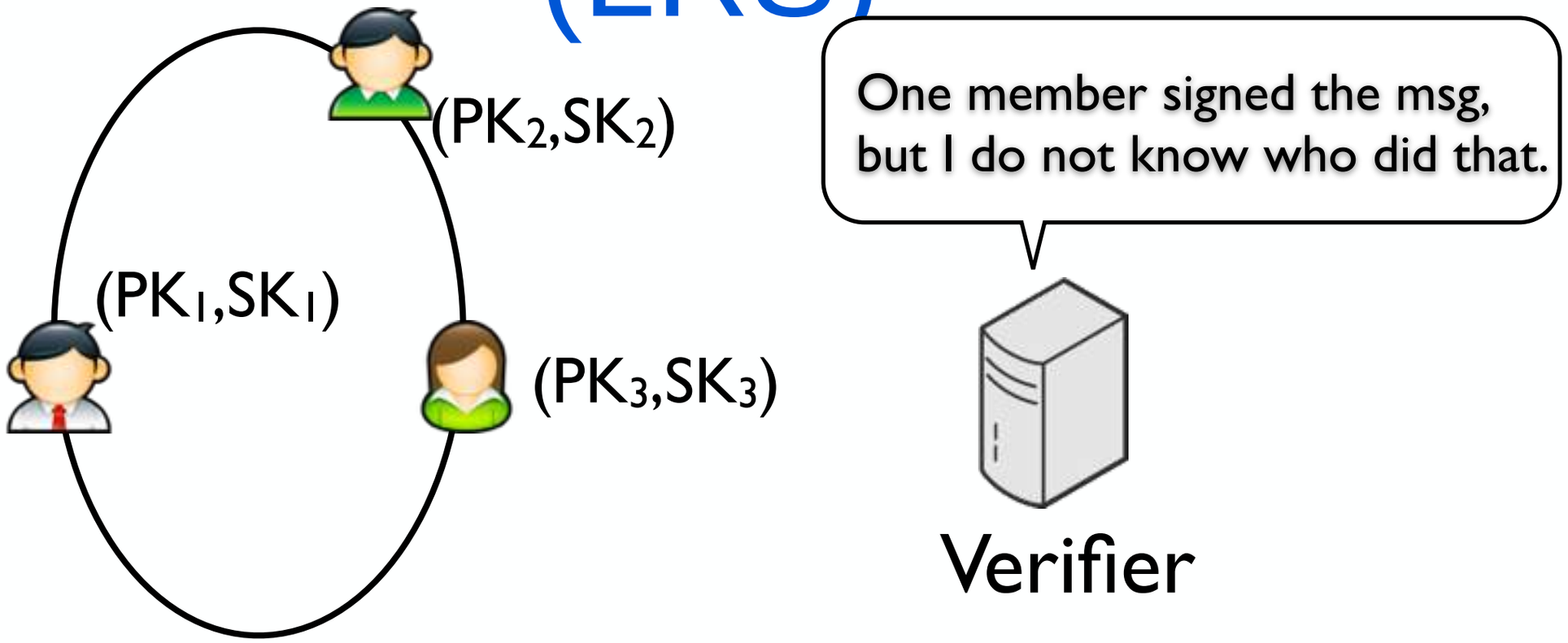
Linkable Ring Signature (LRS)



- LRS can hide voter's pseudonym

* Liu et al. Linkable ring signatures: Security models and new schemes. In ICCSA'05.

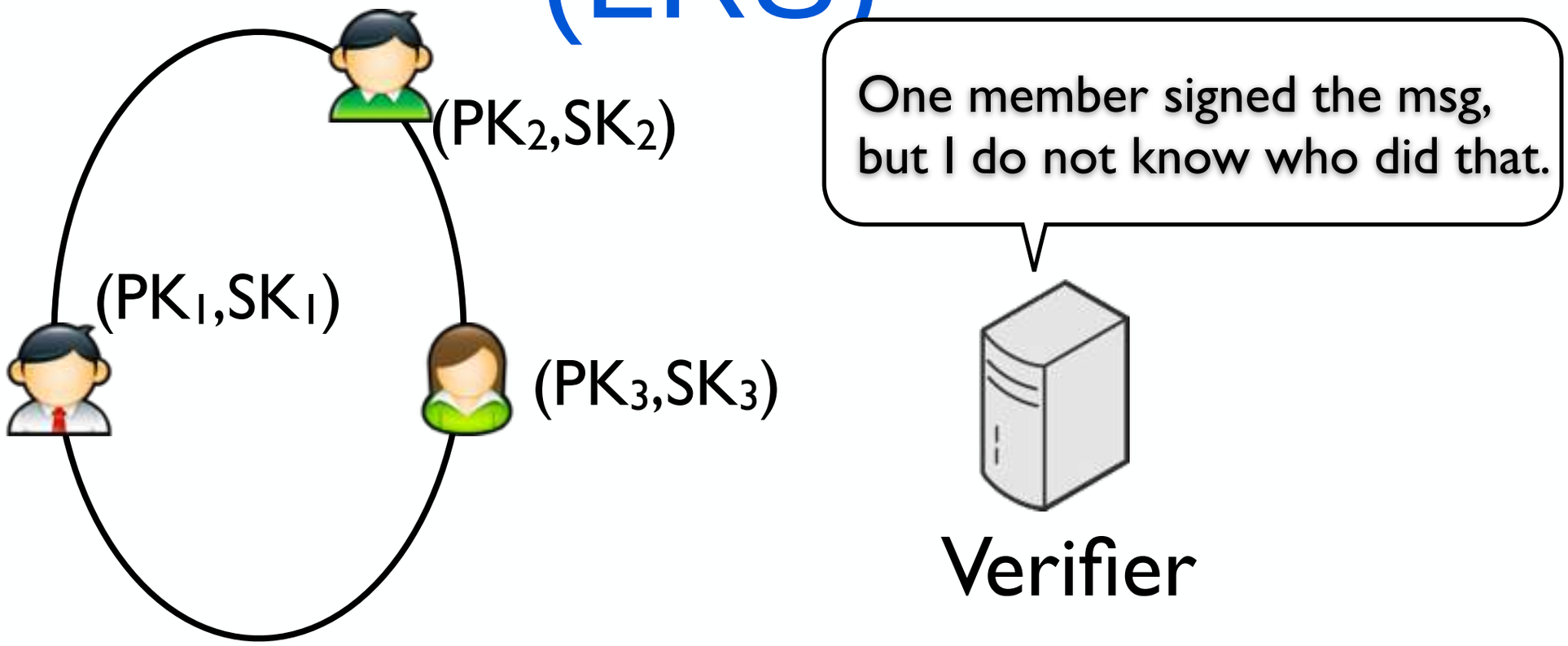
Linkable Ring Signature (LRS)



- LRS can hide voter's pseudonym
- LRS can avoid duplicate votes

* Liu et al. Linkable ring signatures: Security models and new schemes. In ICCSA'05.

Linkable Ring Signature (LRS)



- LRS can hide voter's pseudonym
- LRS can avoid duplicate votes
- Different messages have different LRS

* Liu et al. Linkable ring signatures: Security models and new schemes. In ICCSA'05.

Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	Like: 2 Dislike: 1
Msg2	Hello	Nym_A	2	Like: 1
…	…	…	…	

Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	Like: 2 Dislike: 1
Msg2	Hello	Nym_A	2	Like: 1
…	…	…	…	

AnonRep supports diverse reputation algorithms

Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	3	Like: 2 Dislike: 1
Msg2	Hello	Nym_A	2	Like: 1
…	…	…	…	

3+2-1=4

2+1=3

Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	4	Like: 2 Dislike: 1
Msg2	Hello	Nym_A	3	Like: 1
…	…	…	…	

3+2-1=4

2+1=3

Nym_B's reputation becomes 4

Nym_A's reputation becomes 3

Step3: Feedback Collection

MsgID	Msg	User	Score	Votes
Msg1	Hi	Nym_B	4	Like: 2 Dislike: 1
Msg2	Hello	Nym_A	3	Like: 1
…	…	…	…	

3+2-1=4

2+1=3

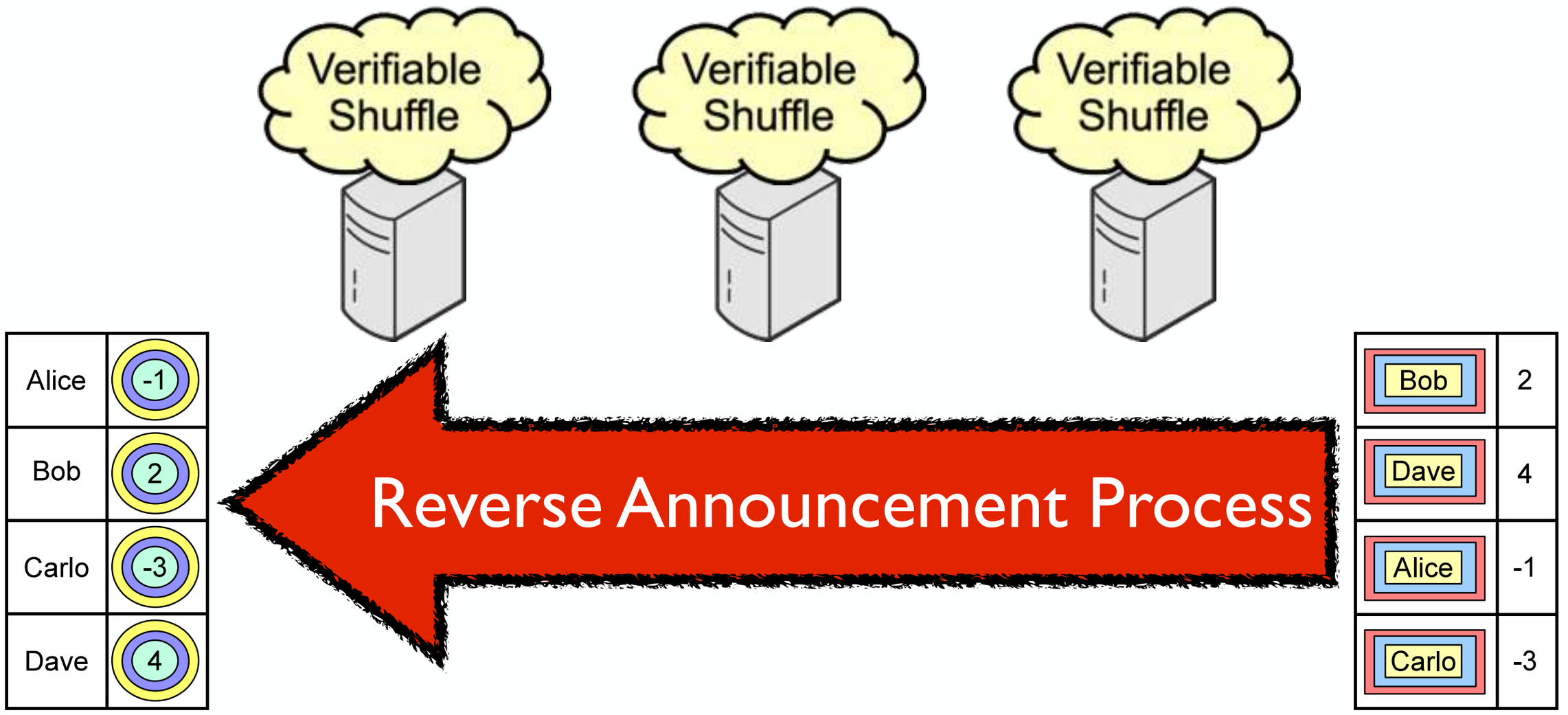
Fresh Nym list with updated reputation

Step3: Feedback Collection

Bob	2
Dave	4
Alice	-1
Carlo	-3

Updated Fresh Nym List

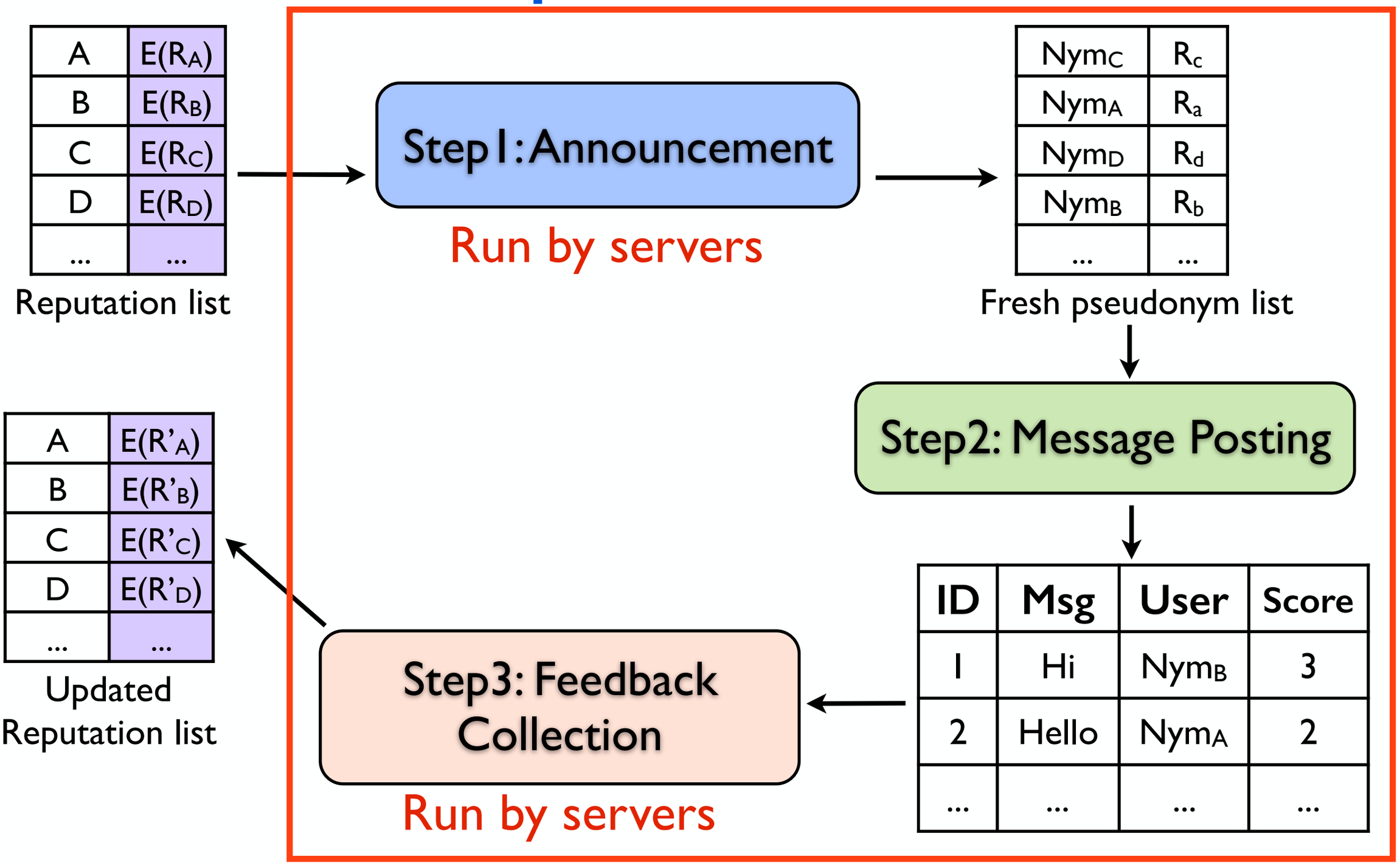
Step3: Feedback Collection



Updated Reputation List

Updated Fresh Nym List

Three Steps in Each Round



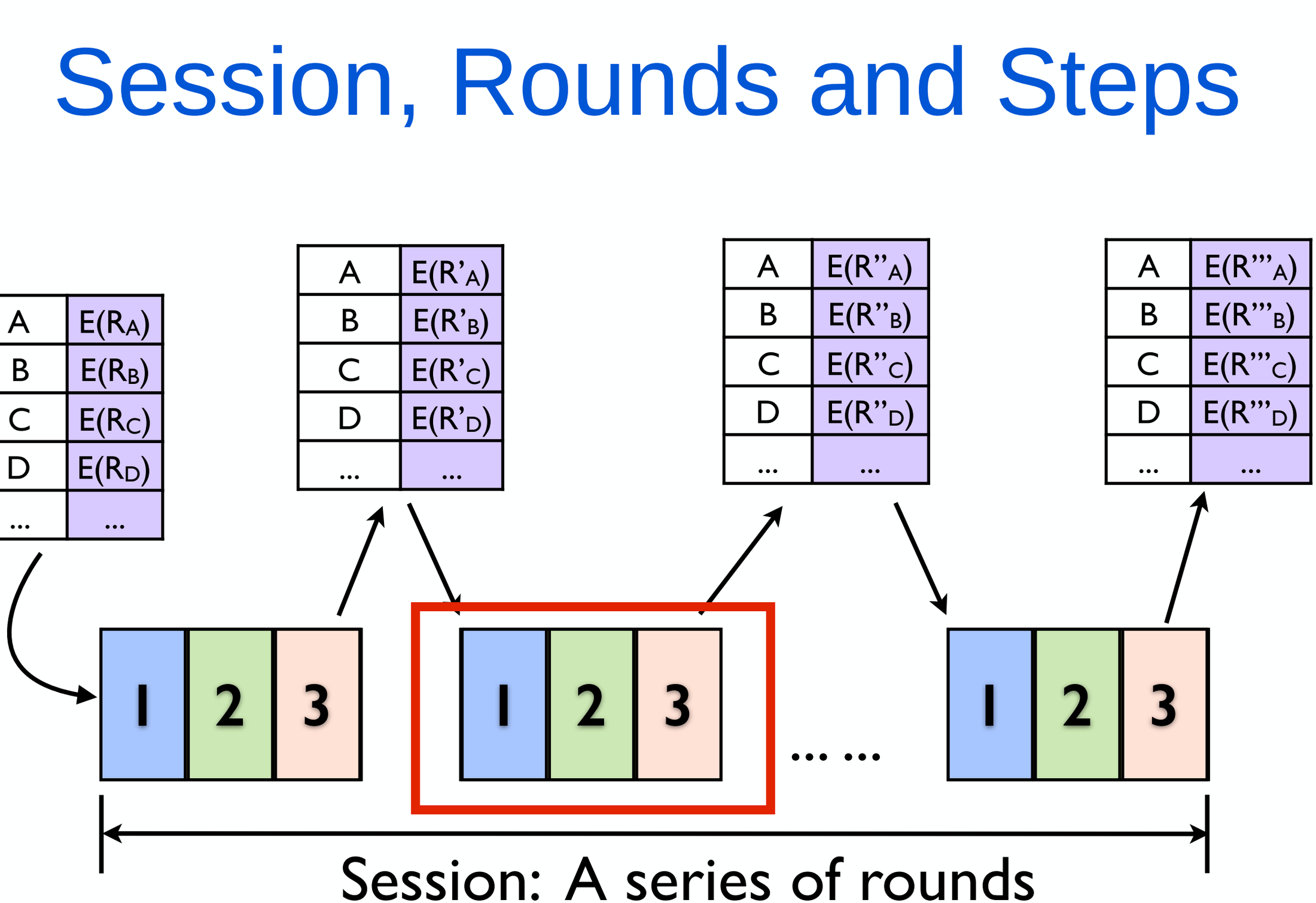
Session, Rounds and Steps

A	$E(R_A)$
B	$E(R_B)$
C	$E(R_C)$
D	$E(R_D)$
...	...

A	$E(R'_A)$
B	$E(R'_B)$
C	$E(R'_C)$
D	$E(R'_D)$
...	...

A	$E(R''_A)$
B	$E(R''_B)$
C	$E(R''_C)$
D	$E(R''_D)$
...	...

A	$E(R'''_A)$
B	$E(R'''_B)$
C	$E(R'''_C)$
D	$E(R'''_D)$
...	...



Road-Map

- Motivations
- AnonRep Design
- Practical Considerations
- Evaluation

Practical Considerations

- Intersection attacks on special reputations
- Performance optimization
- Misbehavior detection
- Registration verification

Practical Considerations

- Intersection attacks on special reputations
- Performance optimization
- Misbehavior detection
- Registration verification

Please see our paper for more details

Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	... ...	...

Round *i*

Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	... ...	...

Round *i*

Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	... ...	...

Round *i*

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(101)	like:0 dislike:1
...	... ...	...

Round *i*+*1*

Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	... ...	...

Round *i*

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(101)	like:0 dislike:1
...	... ...	...

Round *i*+*1*

Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	... ...	...

Round *i*

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(101)	like:0 dislike:1
...	... ...	...

Round *i*+*1*

Msg7	829q(-2)	like:1 dislike:1
Msg8	fapqx(100)	like:3 dislike:2
Msg9	zcvbfa(2)	like:1 dislike:2
...	... ...	...

Round *i*+2

Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	... ...	...

Round *i*

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(101)	like:0 dislike:1
...	... ...	...

Round *i*+*1*

Msg7	829q(-2)	like:1 dislike:1
Msg8	fapqx(100)	like:3 dislike:2
Msg9	zcvbfa(2)	like:1 dislike:2
...	... ...	...

Round *i*+2

Intersection Attack

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	... ...	...

Round *i*

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(101)	like:0 dislike:1
...	... ...	...

Round *i*+*1*

Msg7	829q(-2)	like:1 dislike:1
Msg8	fapqx(100)	like:3 dislike:2
Msg9	zcvbfa(2)	like:1 dislike:2
...	... ...	...

Round *i*+2

Security-Enhanced AnonRep

Security-Enhanced AnonRep

- Actual reputation scores are maintained as ciphertexts
- Solution: Homomorphic encryption [1]

[1] Cramer et al. A secure and optimally efficient multi-authority election scheme. In EUROCRYPT'97.

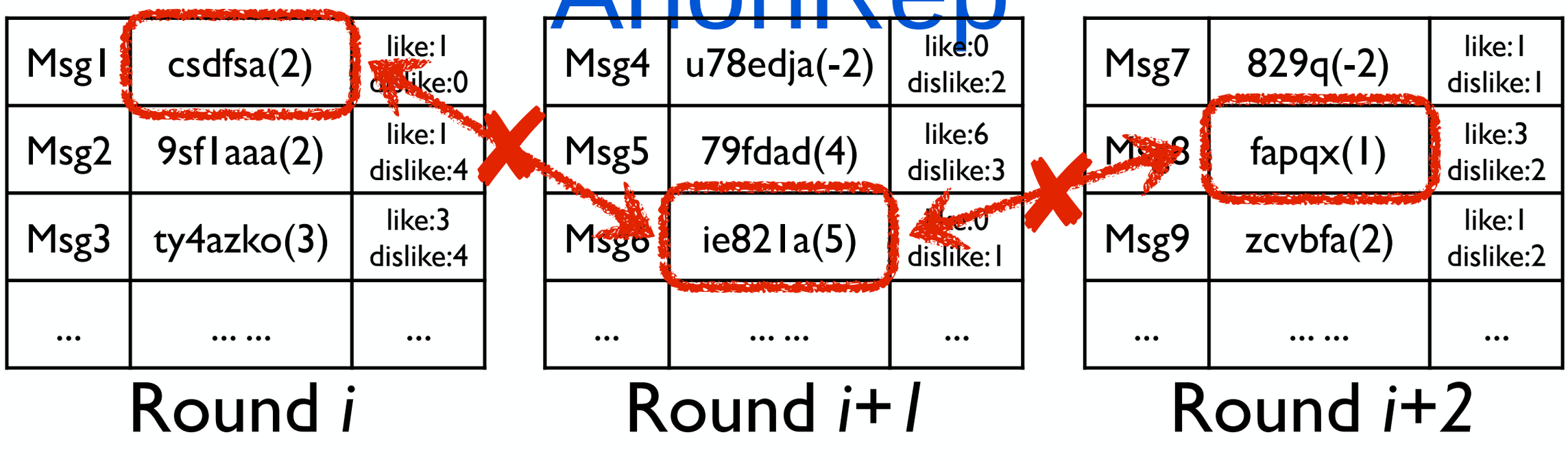
Security-Enhanced AnonRep

- Actual reputation scores are maintained as ciphertexts
- Solution: Homomorphic encryption [1]
- Reputation budget: posting message with budget < actual score
- Solution: Zero-knowledge proof [2]

[1] Cramer et al. A secure and optimally efficient multi-authority election scheme. In EUROCRYPT'97.

[2] Camenisch et al. Proof systems for general statements about discrete logarithms. In ETH TR'97.

Security-Enhanced AnonRep



Security-Enhanced AnonRep

Msg1	csdfsa(2)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	... ...	...

Round *i*

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(5)	dislike:1
...	... ...	...

Round *i+1*

Msg7	829q(-2)	like:1 dislike:1
Msg8	fapqx(1)	like:3 dislike:2
Msg9	zcvbfa(2)	like:1 dislike:2
...	... ...	...

Round *i+2*

V.S.

Msg1	csdfsa(100)	like:1 dislike:0
Msg2	9sf1aaa(2)	like:1 dislike:4
Msg3	ty4azko(3)	like:3 dislike:4
...	... ...	...

Round *i*

Msg4	u78edja(-2)	like:0 dislike:2
Msg5	79fdad(4)	like:6 dislike:3
Msg6	ie821a(101)	dislike:1
...	... ...	...

Round *i+1*

Msg7	829q(-2)	like:1 dislike:1
Msg8	fapqx(100)	like:3 dislike:2
Msg9	zcvbfa(2)	like:1 dislike:2
...	... ...	...

Round *i+2*

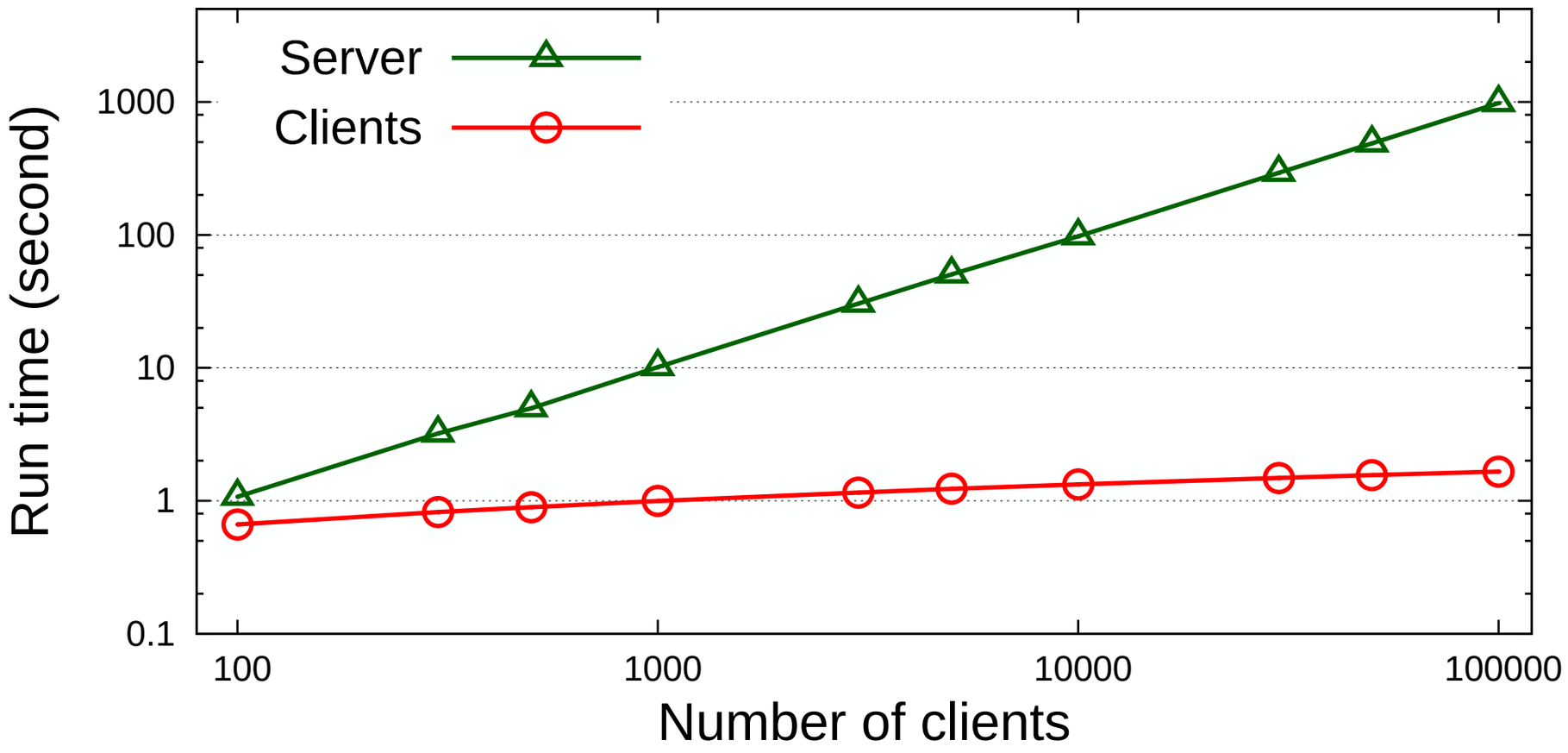
Road-Map

- Motivations
- AnonRep Design
- Practical Considerations
- Evaluation

Implementation

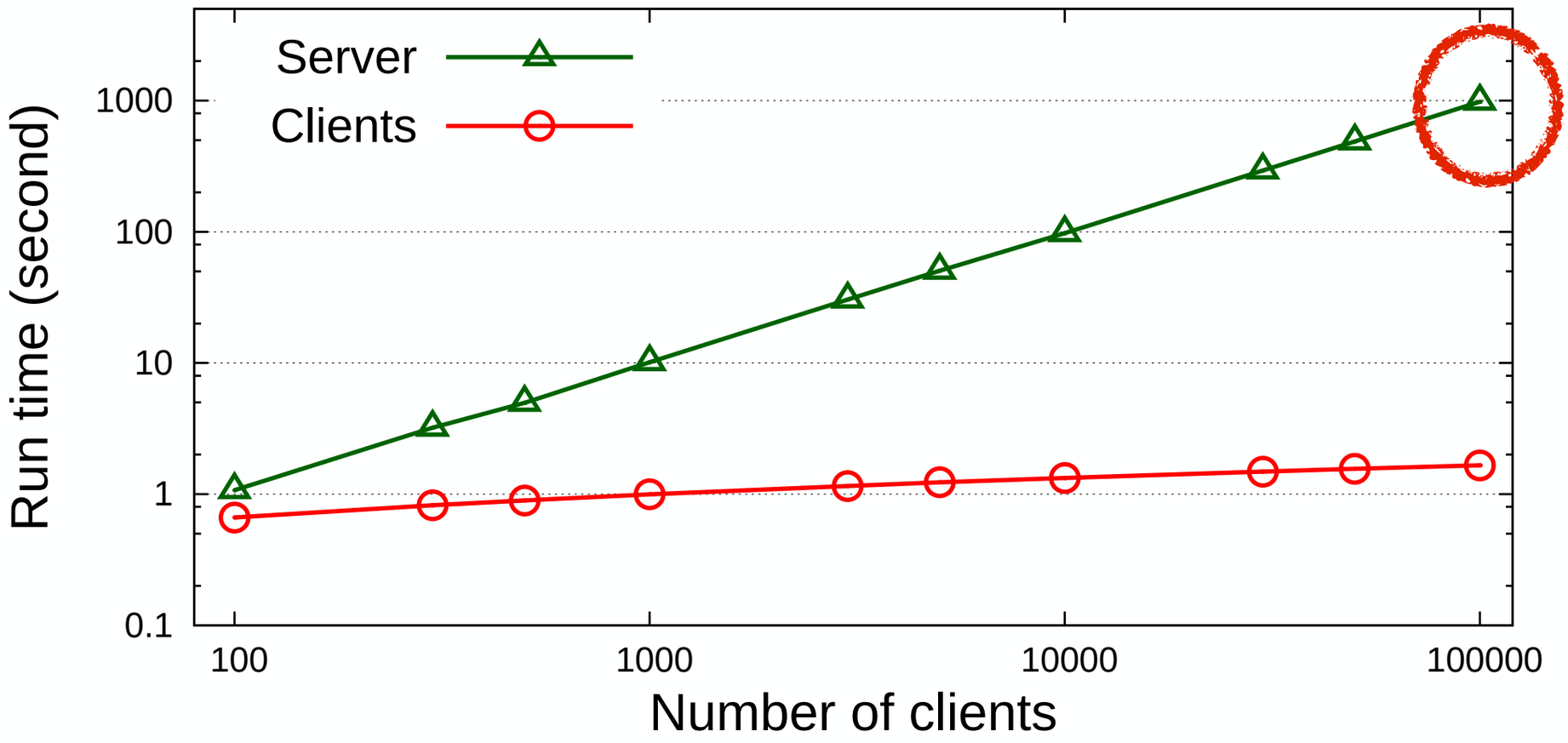
- A working prototype in Go Language
  - Heavily depends on DeDiS Crypto Go library
    https://github.com/DeDiS/crypto
  - Our prototype is open source
    https://github.com/anonyreputation/anonCred

Evaluation



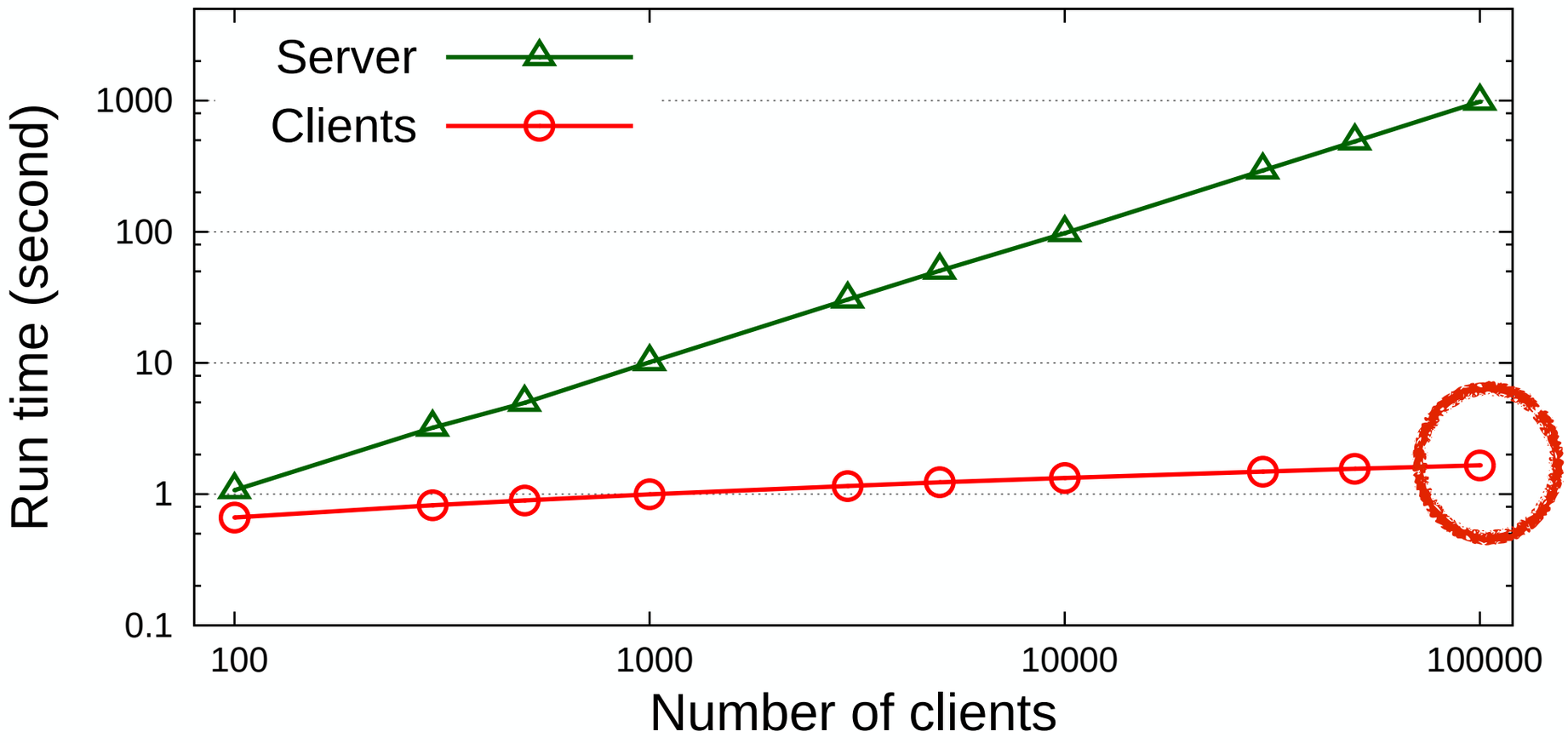
Computational overhead in announcement step

Evaluation



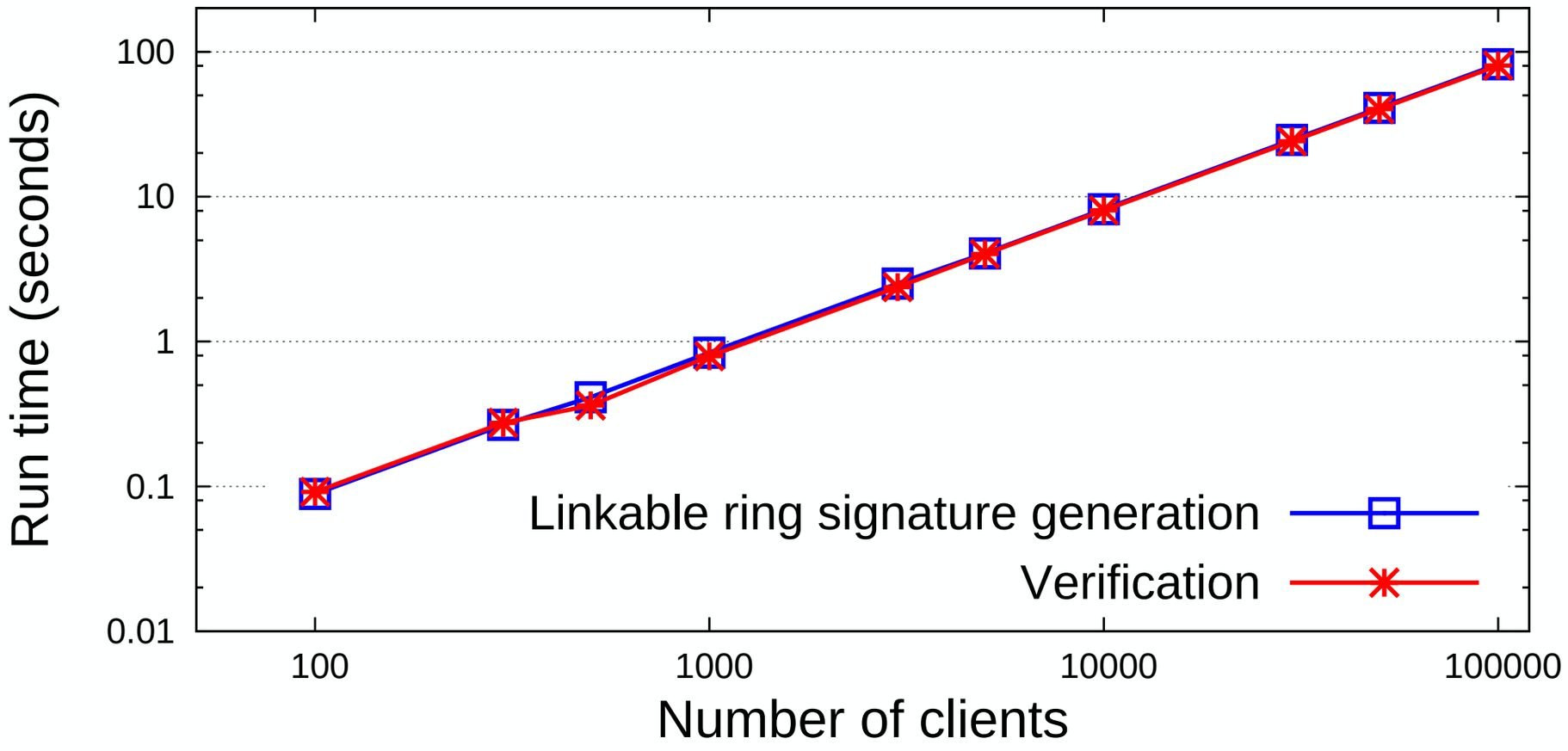
Computational overhead in announcement step

Evaluation



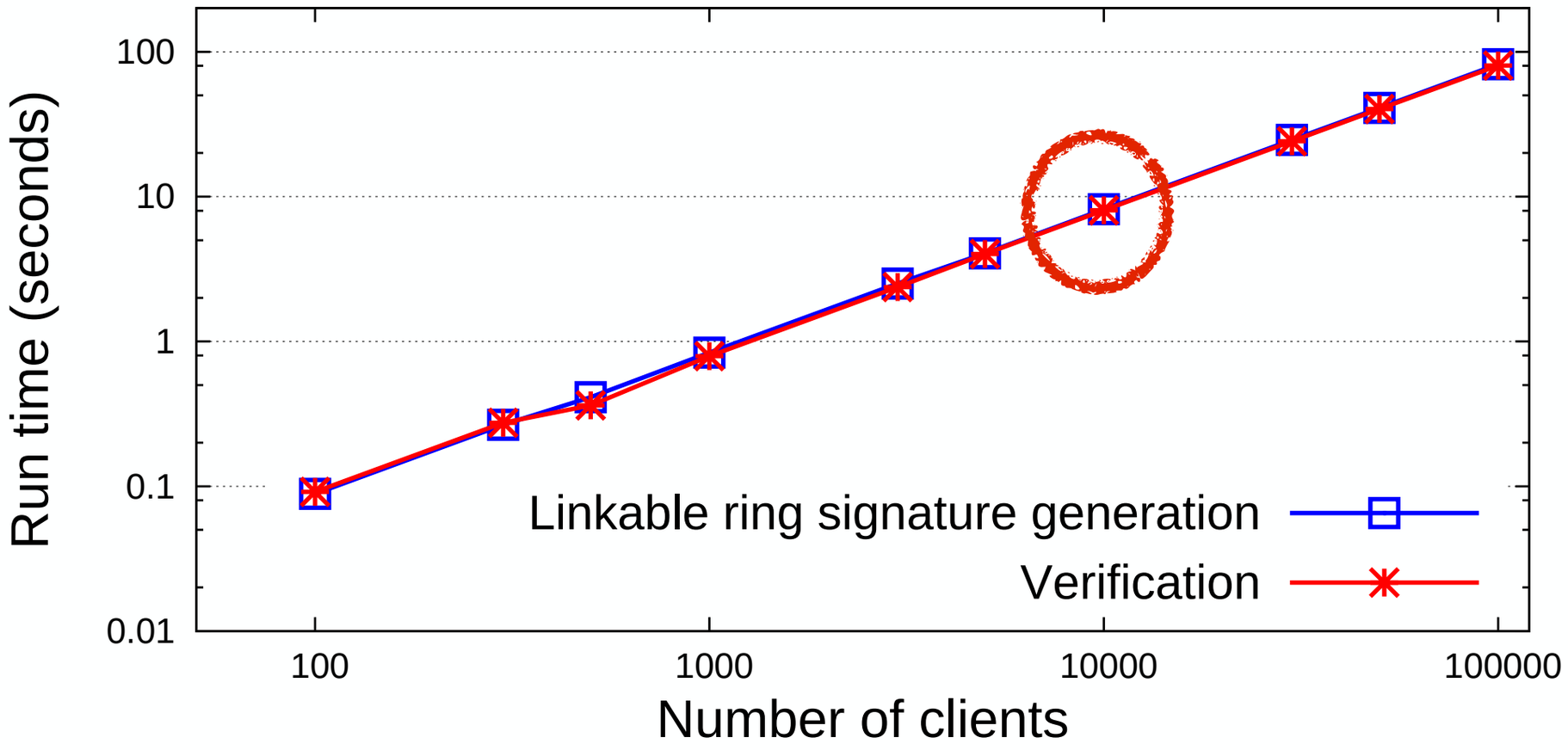
Computational overhead in announcement step

Evaluation



Computational overhead of feedback step

Evaluation



Computational overhead of feedback step

Conclusion

- The first practical tracking-resistant anonymous reputation system:
  - Unlinkability and anonymity of users' activities
  - Diverse reputation utilities (algorithms)
  - No need trust any centralized party
  - Scalable to large-size user set

- Find out more at:
  - http://dedis.cs.yale.edu/dissent/

Collective Authorities: Transparency and Decentralized Trust at Scale

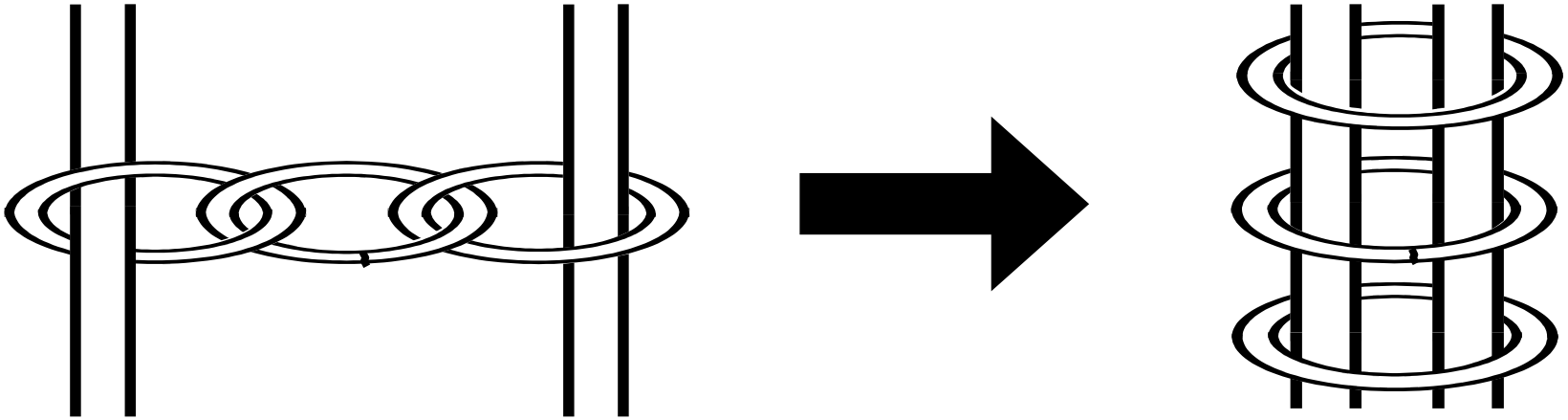
Bryan Ford
DEDIS – Decentralized/Distributed Systems Laboratory
Swiss Federal Institute of Technology in Lausanne (EPFL)

working with many colleagues at Yale and EPFL

FOSAD – Bertinoro, Italy – August 30, 2016

Talk Outline

- **Lessons from building decentralized anonymity systems**
- The need for decentralized authorities
- Baby step: decentralized witness cosigning with CoSi
- Baby step: decentralized public randomness
- Next step: scalable consistent blockchains with ByzCoin
- Conclusion: can decentralization survive the fake people?



Decentralized Systems

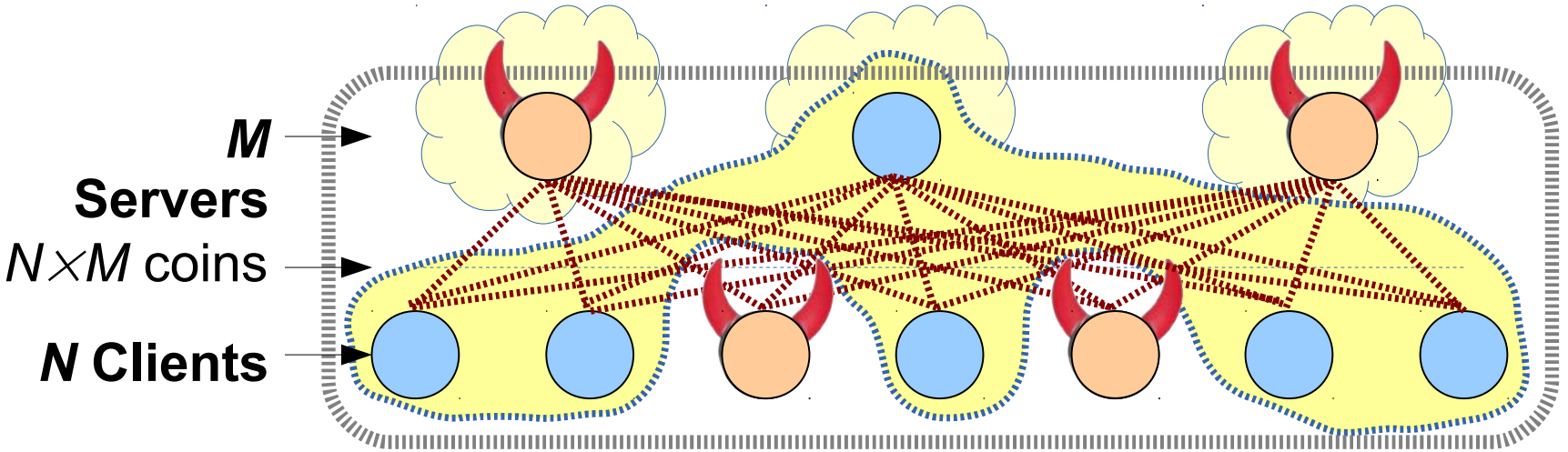
Where everybody can’t quite

“just get along”

Recall: an Elephant in the Room

Dissent – and many other crypto-heavy systems – assumes “a few servers” fall from the sky…

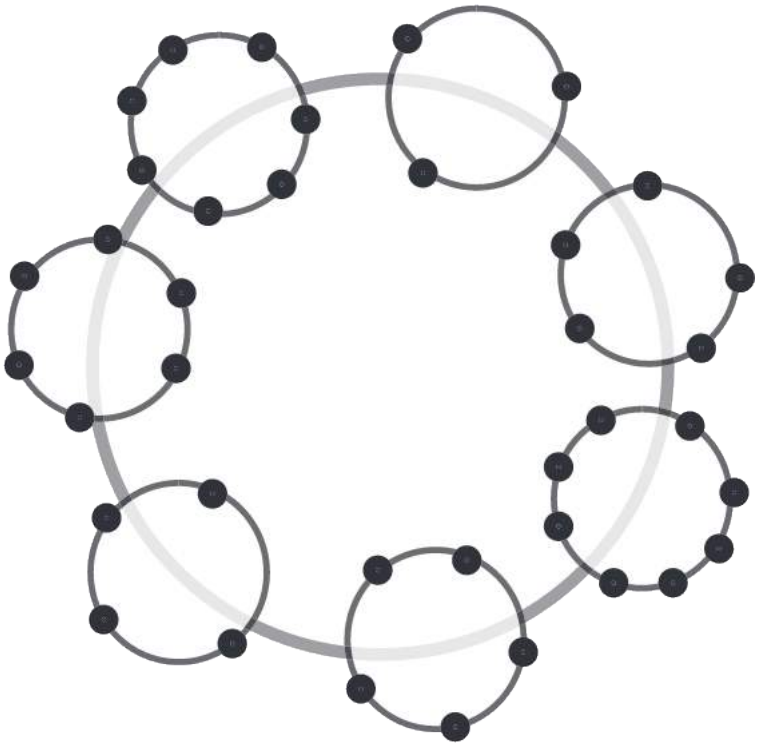
- Only one (unknown) server needs to be honest
- But who chooses the servers? From what list?
- How can we trust that they are “fairly” chosen?



Remember Herbivore?

Achieved scalability by breaking large networks into manageable *k*-anonymity sets

- Those sets were too small (~10s); Dissent etc can fix that
- But we still need "manageable groups" to scale to millions



Key challenge: **how?**

- Who chooses the groups, from what list, and can trust them?

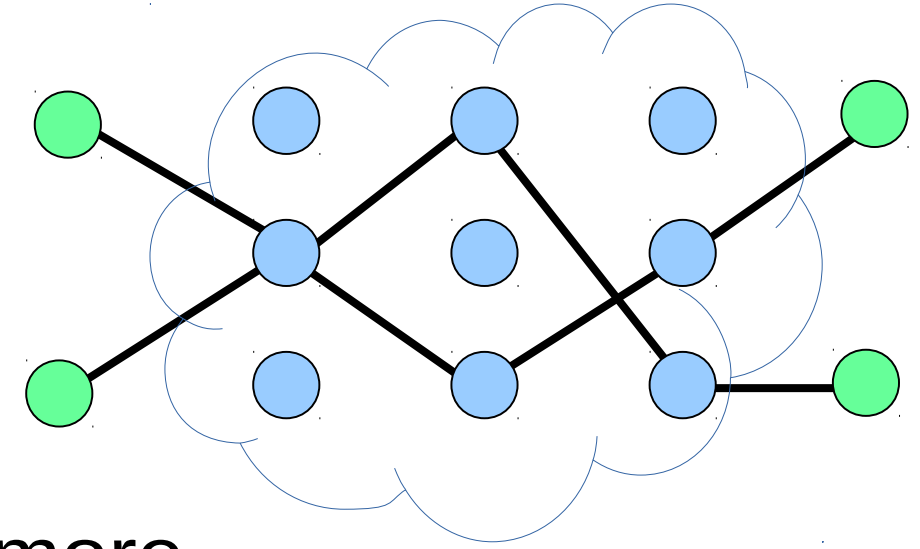
A challenge not unique to Dissent

Common to *all* recent “provable anonymity” systems…

- **Dissent** – Wolinsky et al, CCS 10, OSDI 2012
- **Aqua** – Le Blond et al, SIGCOMM 2013
- **CoinShuffle** – Ruffing et al, ESORICS 2014
- **Riposte** – Corrigan-Gibbs et al, Oakland 2015
- **Baffle** – Zamani et al, ICDCS 2015
- **Herd** – Le Blond et al, SIGCOMM 2015
- **Vuvuzela** – van den Hoof et al, SOSP 2015
- **Riffle** – Kwon et al, PETS 2016

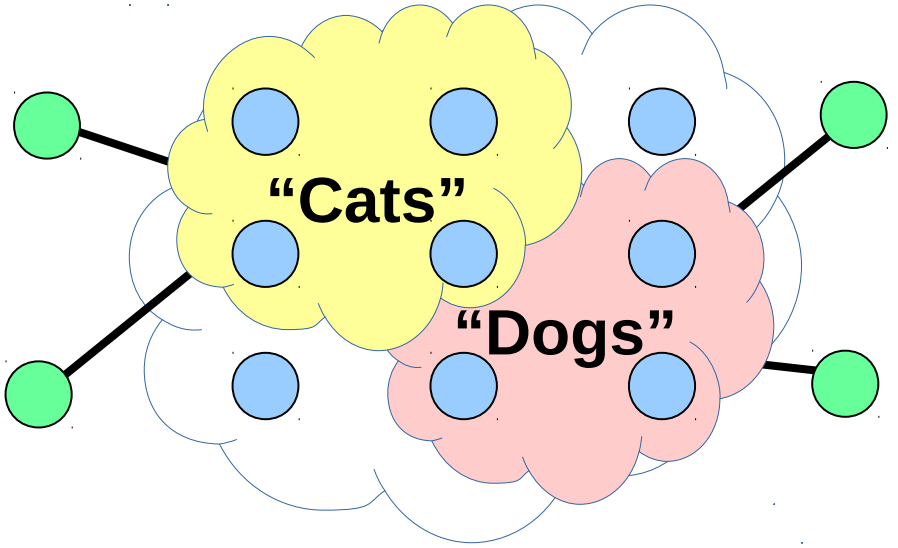
All work, scale “to a point”…

Tor scales because everyone makes **individual choices**



Strong anonymity needs more **global agreement**

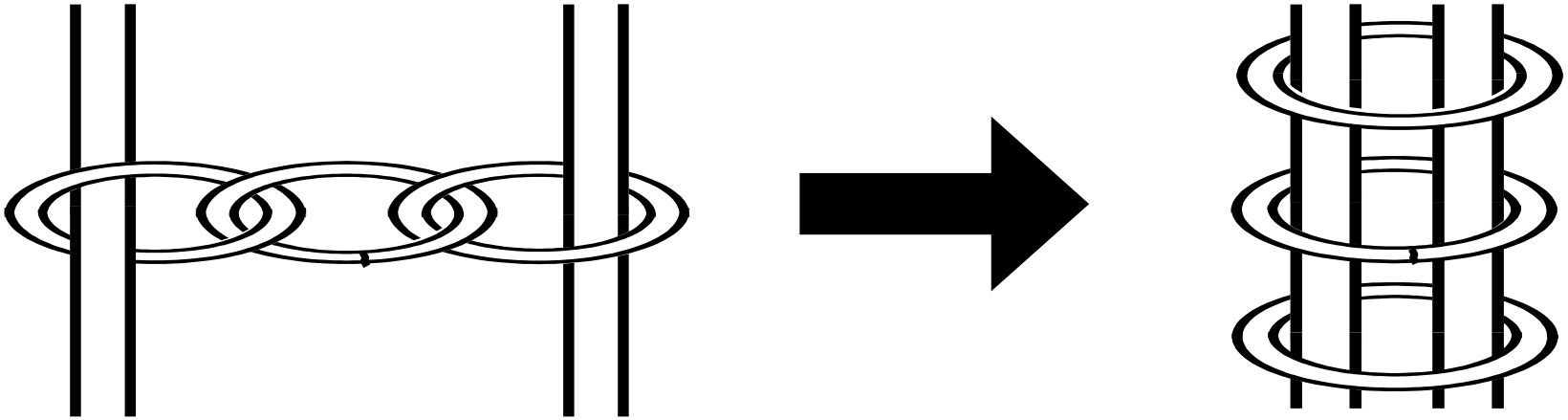
- Particular servers to support chatroom, anonymity set, …



Need an “**Authority**”?

Talk Outline

- Lessons from building decentralized anonymity systems
- **The need for decentralized authorities**
- Baby step: decentralized witness cosigning with CoSi
- Baby step: decentralized public randomness
- Next step: scalable consistent blockchains with ByzCoin
- Conclusion: can decentralization survive the fake people?



Dependence on critical authorities

Conceptually simple but **security-critical** services

- Time Services (NTP)

- Digital Notaries

- Naming Authorites

SECURE64

- Certificate Authorities

- Randomness Authorities (e.g., Lotteries)

- Software Update Services

Are Internet authorities trustworthy?

WIRED Hack Obtains 9 Bogus Certificates for Prominent ...

HACK OBTAINS 9 BOGUS CERTIFICATES FOR PROMINENT WEBSITES; TRACED TO IRAN

Are Internet authorities trustworthy?

CYBER CRIME SCAMS AND FRAUD

This Dude Hacked Lottery Computers To Win $14.3M Jackpot In U.S.

By Waqas on April 14, 2015 *Email* *@hackread*

Are Internet authorities trustworthy?

threatpost CATEGORIES FEATURED PODCASTS VIDEOS

10/08/15 5:54

Advanced notice: Security updates for Adobe Acrobat and Reader are due on Patch Tuesday: https://t.co/QLqnpulr0A

Welcome > Blog Home > Cryptography > D-Link Accidentally Leaks Private Code-Signing Keys

by Michael Mimoso Follow @mike_mimoso

September 18, 2015 , 10:21 am

Are Internet authorities trustworthy?

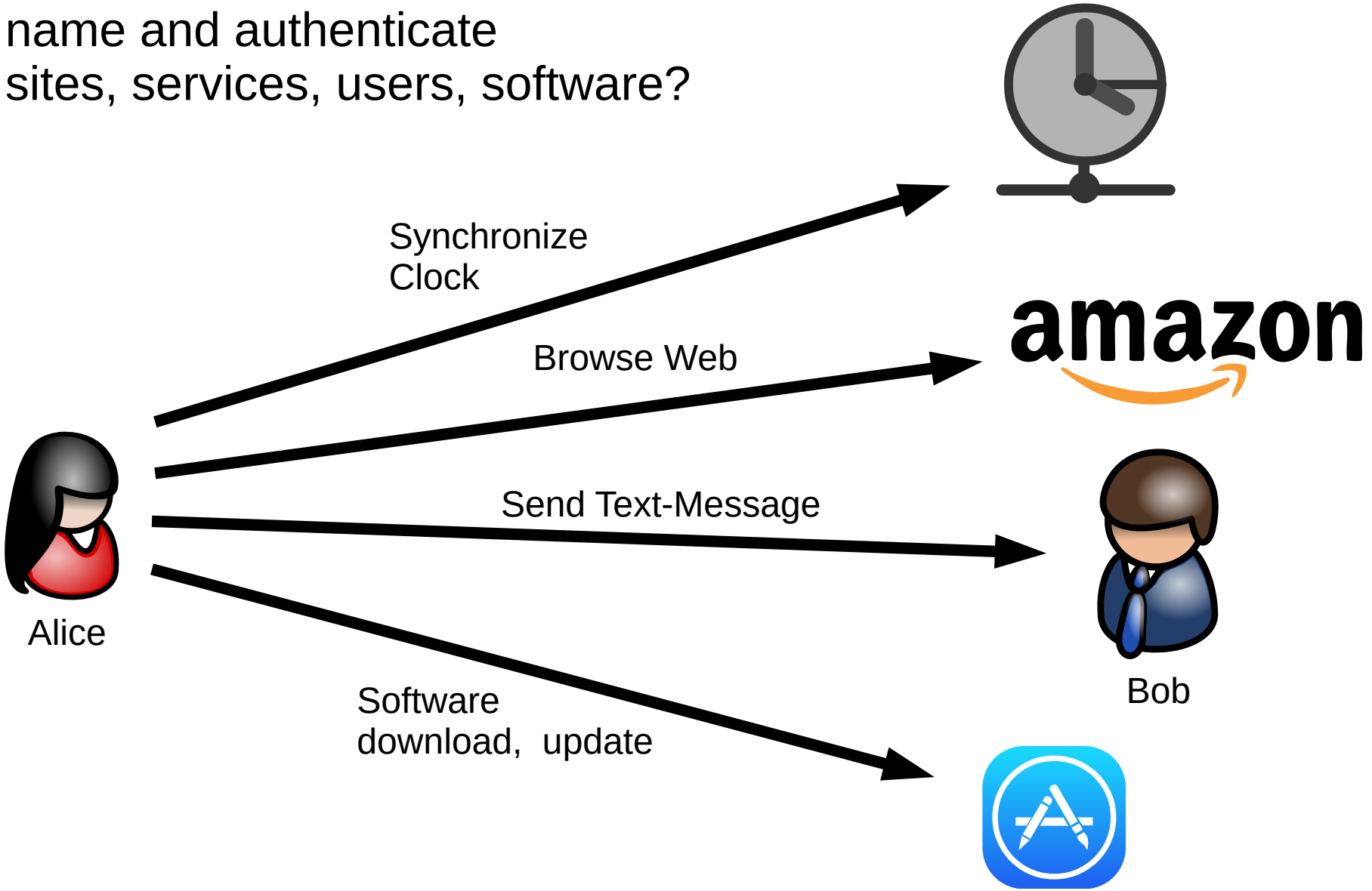
New attacks on Network Time Protocol can defeat HTTPS and create chaos

Exploits can be used to snoop on encrypted traffic and cause debilitating outages.

by **Dan Goodin** - Oct 22, 2015 12:07am CEST

Deep Dependence on Authorities

How does an Internet client
name and authenticate
sites, services, users, software?



Deep Dependence on Authorities

Respect my Authoritah!

?

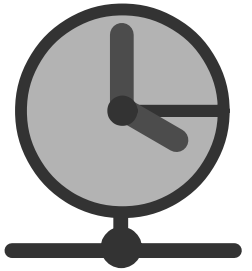
amazon

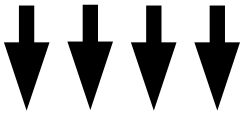
Alice

What is:
- The current time?
- Amazon's SSL public key?
- Bob's IM public key?
- Latest version of App?

Bob

Authorities Make & Sign Statements





“The time is 3PM.”

amazon

“Amazon’s public key is X.”

Alice

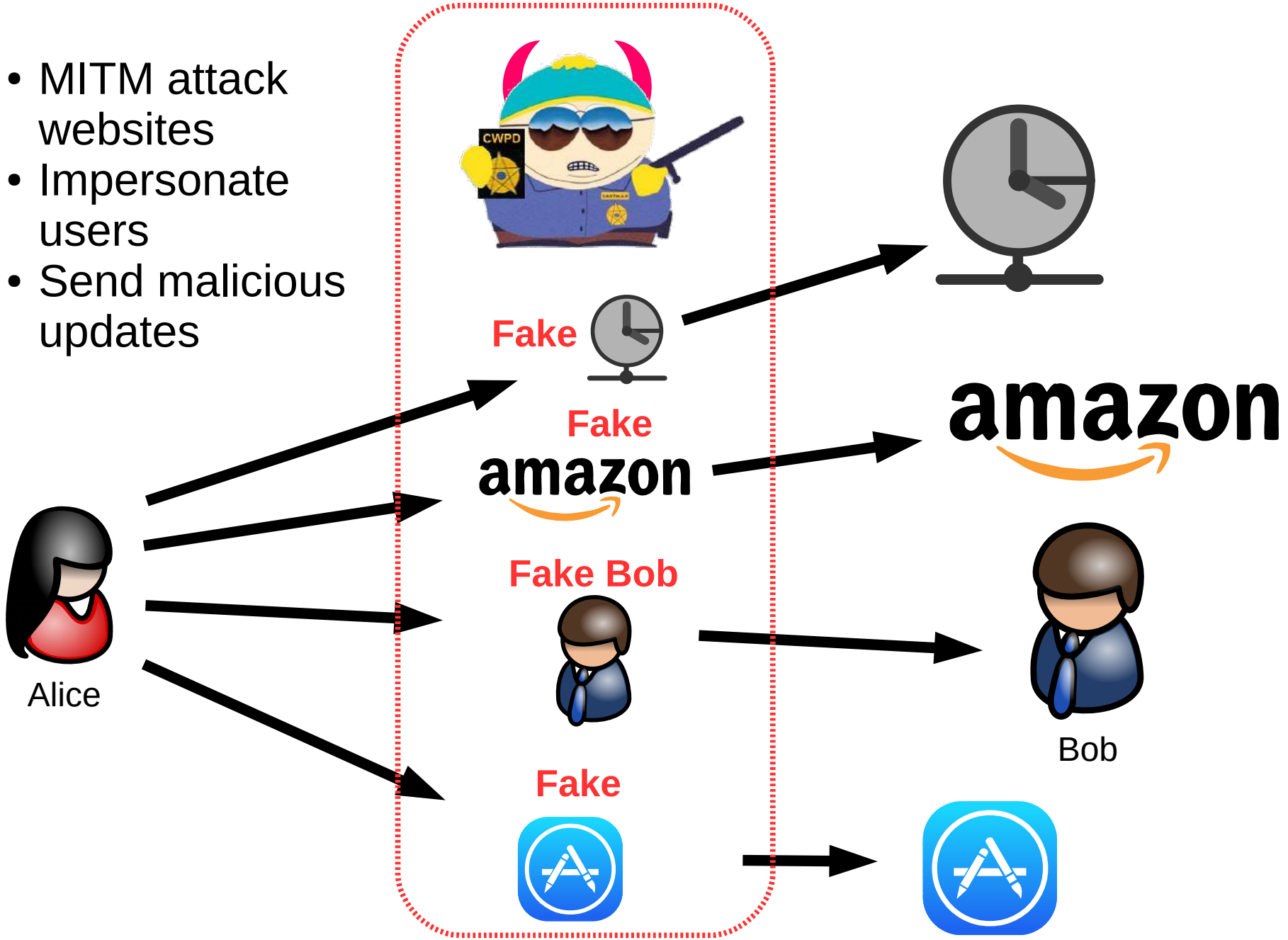
“Bob's public key is Y.”

Bob

“The hash of latest iOS is Z.”

Problem #1: Authority Compromise

- MITM attack websites
- Impersonate users
- Send malicious updates



Problem #2: Weak Links

Clients often depend on **many** authorities: e.g., hundreds of CAs trusted by web browsers

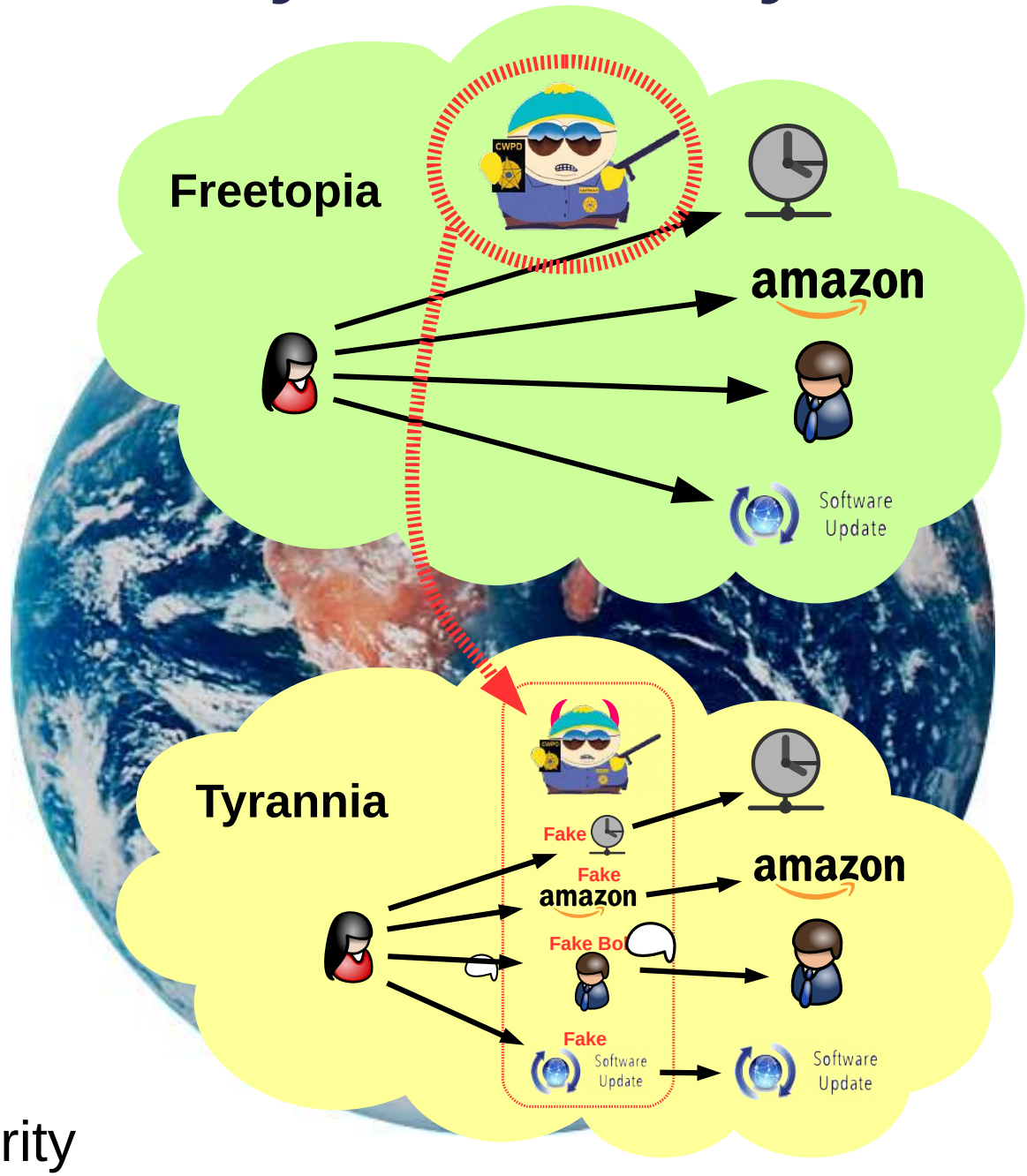
- Any CA can issue cert for any domain name

Attacker often needs to **compromise only one**

- **Weakest-link** security
- @#$% happens
  - DigiNotar, Comodo, CNNIC/MCS

Problem #3: Secret Key Portability

- Attacker need not compromise authority "in-place"
- Instead steal the authority's **secret key**
  - Use it to create an "evil twin" on attacker's turf
  - Avoid detection by confining use to specific targets
  - Block targets from reporting to real authority



Problem #4: Everybody Wants In

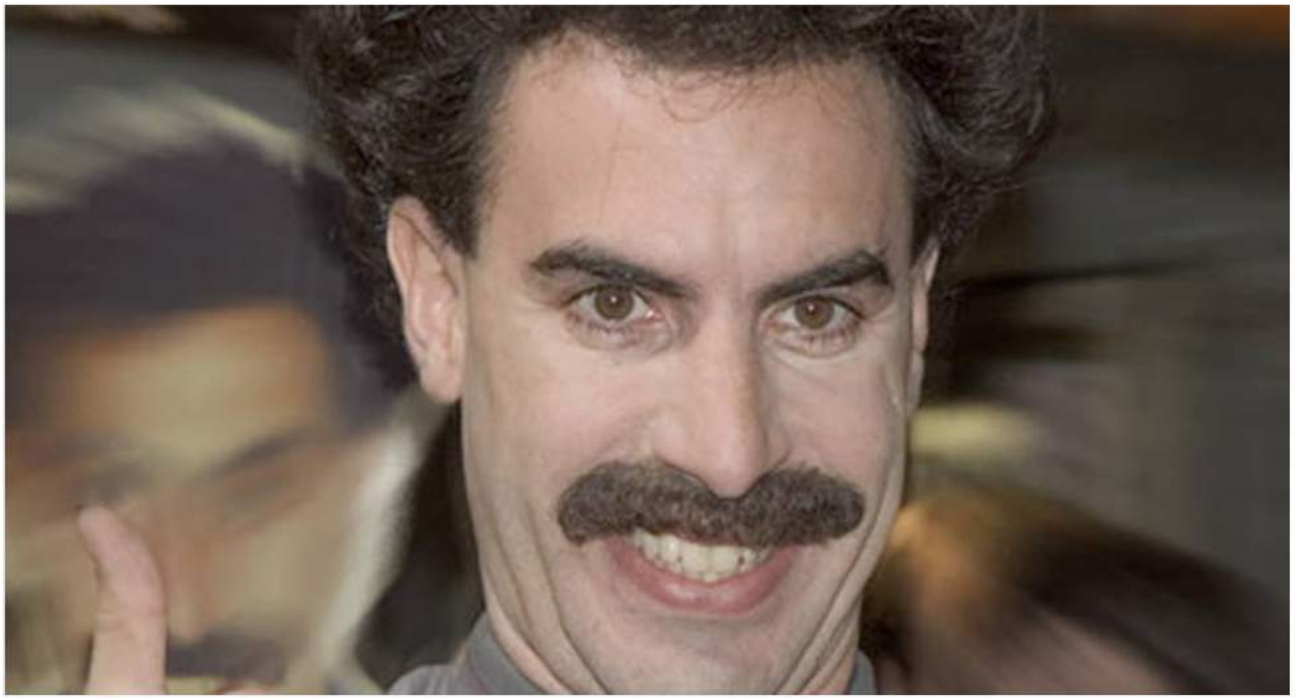
Hackers, organized crime, governments…

The Register®
Biting the hand that feeds IT

Security

Is Kazakhstan about to man-in-the-middle diddle all of its internet traffic with dodgy root certs?

Come on, guys. Don't go giving the Russians any ideas



Problem #4: Everybody Wants In

Hackers, organized crime, governments…

What To Do?

We have to assume that no individual…

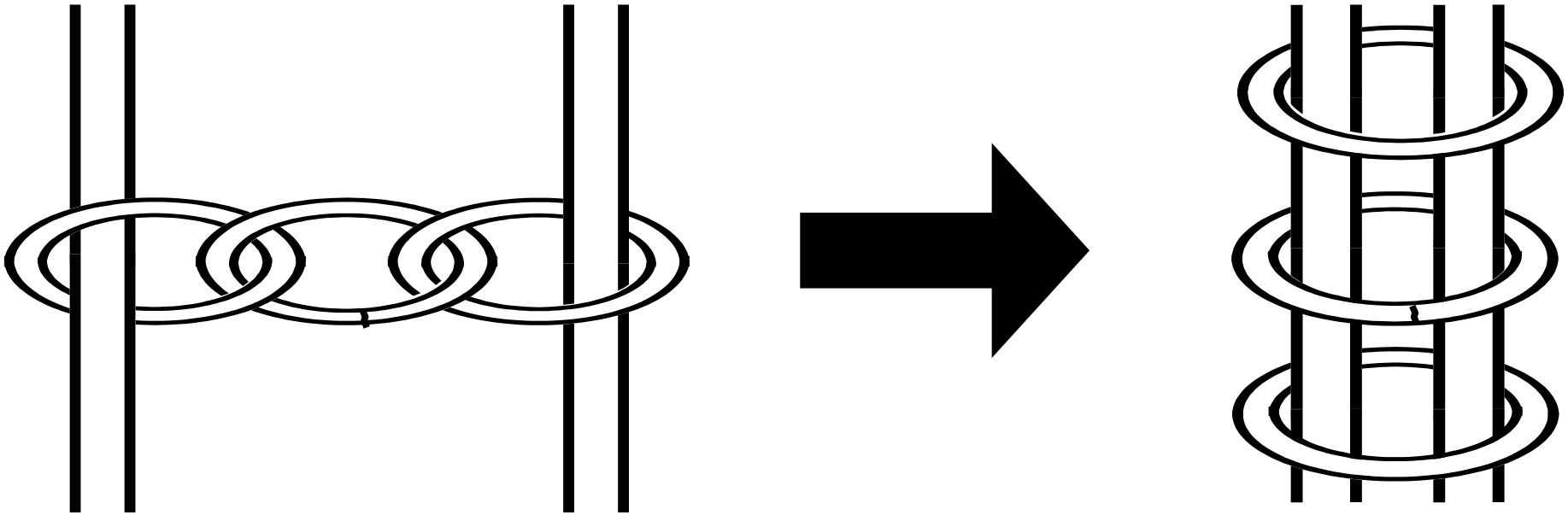
- Hardware platform
- Software system
- System/network administrator
- Authoritative organization

…is invulnerable to compromise (or coercion)

Decentralize the Authorities!

Split trust across independent parties

- So system resists compromise by individuals
- From **weakest-link** to **strongest-link** security
- Decentralized resistance to failure, coercion



Example: Tor Directory Authority

Split across ~10 servers – **but is this enough?**

- Could attacker hack or coerce ~5 operators?

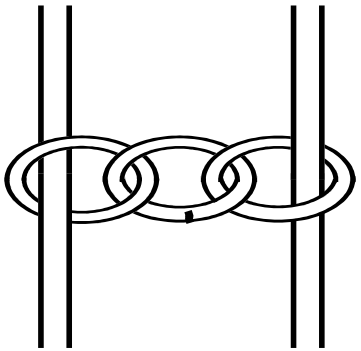
(image credit: Jordan Wright)

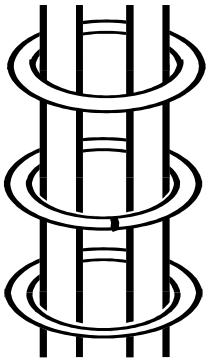
Trust-splitting needs to scale

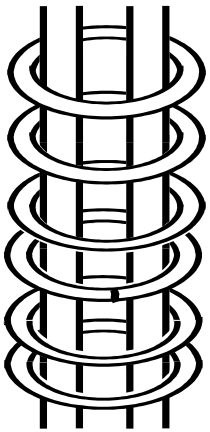
Weakest-link:
T = 1

Strongest-link:
T = 2-10

Collective authorities:
T = 100s,1000s







Trust-splitting needs to scale

Must incorporate **all diversity that makes sense**

- Not just ~10 parties “picked by someone”

Could we decentralize…

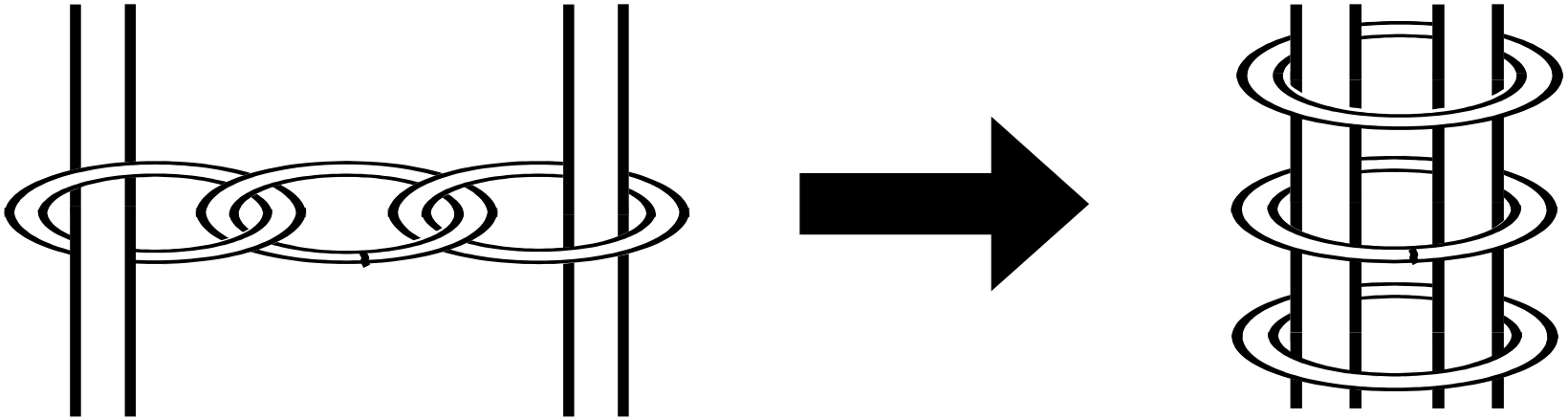
- **TLS certificate validation and signing**
  across the hundreds of certificate authorities?
- **DNSSEC root zone maintenance and signing**
  across the 1000+ worldwide TLD operators?
- **A national cryptocurrency**
  across the thousands of US national banks?

Make overall security **grow** as scale increase?

Not Gonna Happen Overnight…

Talk Outline

- **Lessons from building decentralized anonymity systems**
- The need for decentralized authorities
- **Baby step: decentralized witness cosigning with CoSi**
- Baby step: decentralized public randomness
- Next step: scalable consistent blockchains with ByzCoin
- Conclusion: can decentralization survive the fake people?

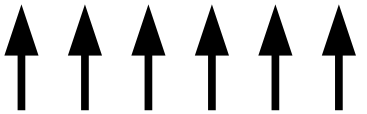


A First Step: **Transparency**

More readily achievable near-term

- Who watches the watchers?
  Public **witnesses**!

Respect my Authoritah!



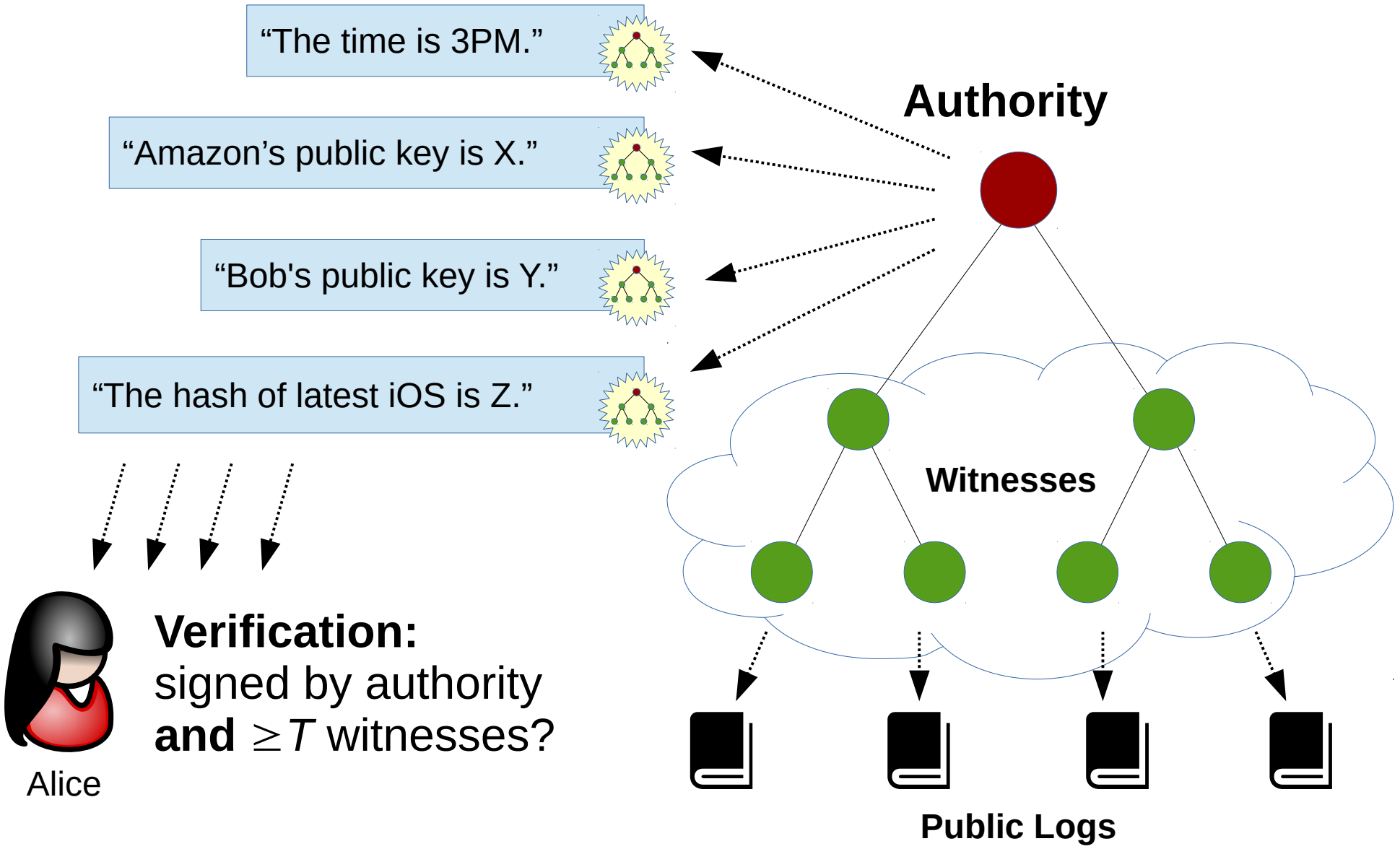
Ensure that **any** authoritative statement:

- Is exposed to **public scrutiny**
- Conforms to **checkable standards**

before clients will accept statement

Key: **practical to "retrofit" existing authorities**

Decentralized Witness Cosigning



Is the Signed Statement "Good"?

In general, **witnesses don't (and can't) know for sure**

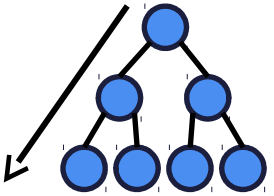
- Does public key X really belong to Bob?
- Does software image Y have a secret backdoor?

But witnesses can still ensure **all signatures are public**

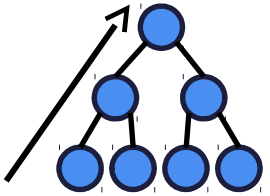
- If authority coerced or its keys used to produce bad statement, attacker can't ensure its secrecy
  - Backdoors possible but must "hide in plain sight"
- Creates "Ulysses Pact" deterrent against coercion
  - "the point…is to keep governments from even trying to put secret pressure on tech companies, because the system is set up so that the secret immediately gets out" - Cory Doctorow, 10-March-2016

CoSi Protocol Signing Rounds

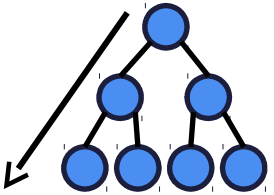
1. Announcement Phase



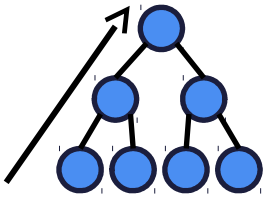
2. Commitment Phase



3. Challenge Phase



4. Response Phase

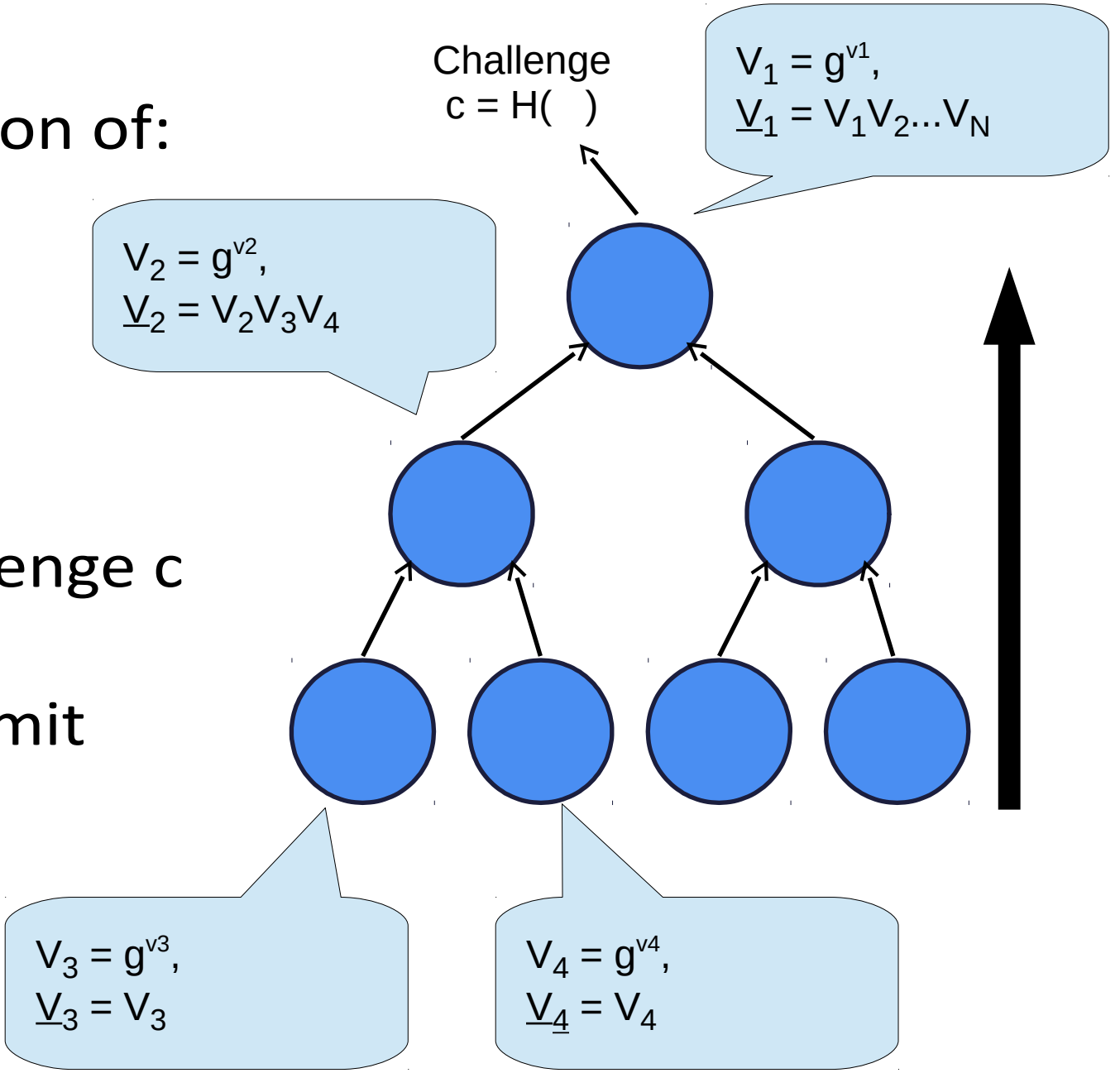


CoSi Commit Phase

Tree computation of:

- Commits V_i
- Aggregate commits $\underline{V}_i$

Collective challenge c is hash of aggregate commit



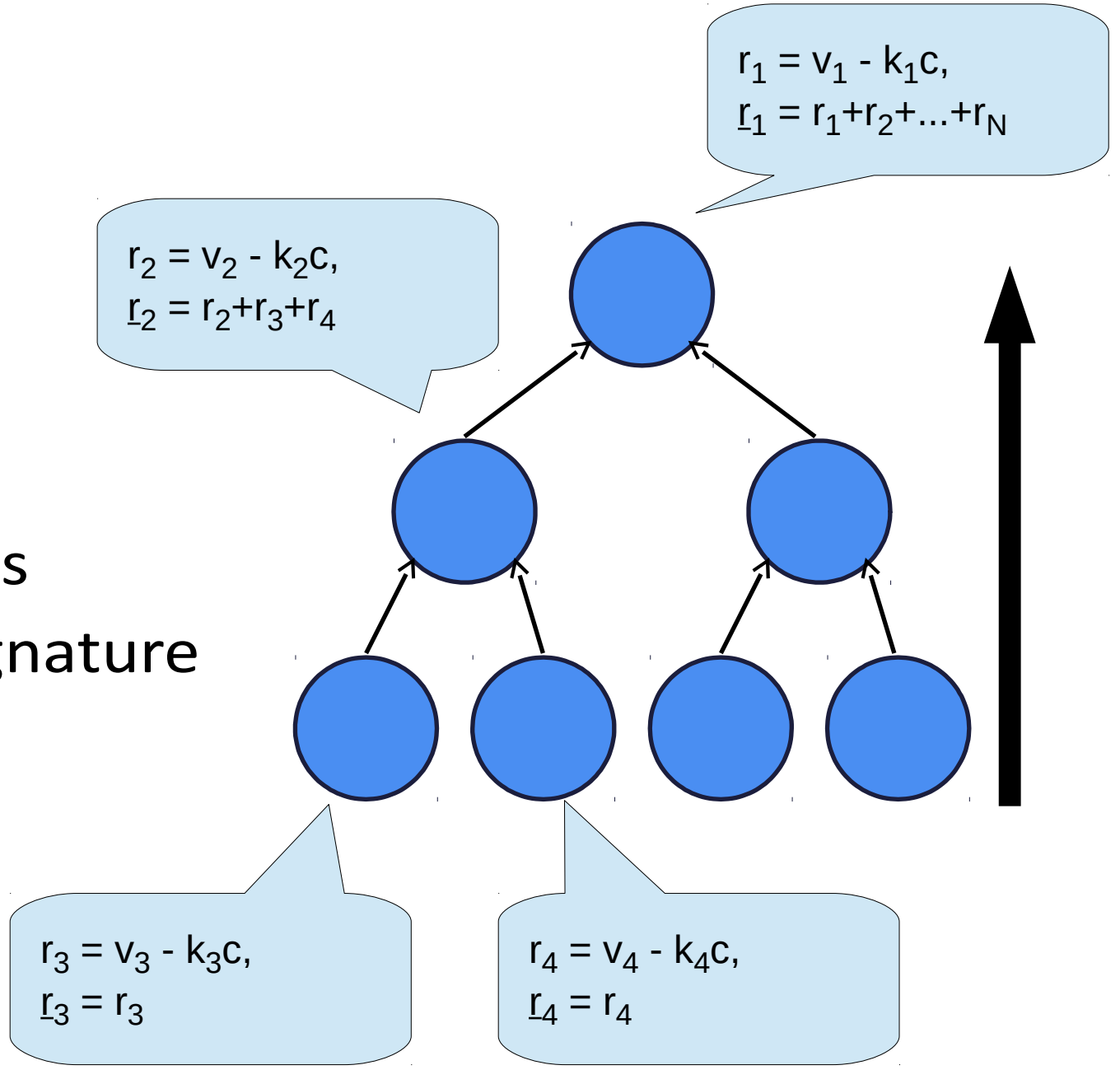
CoSi Response Phase

Compute

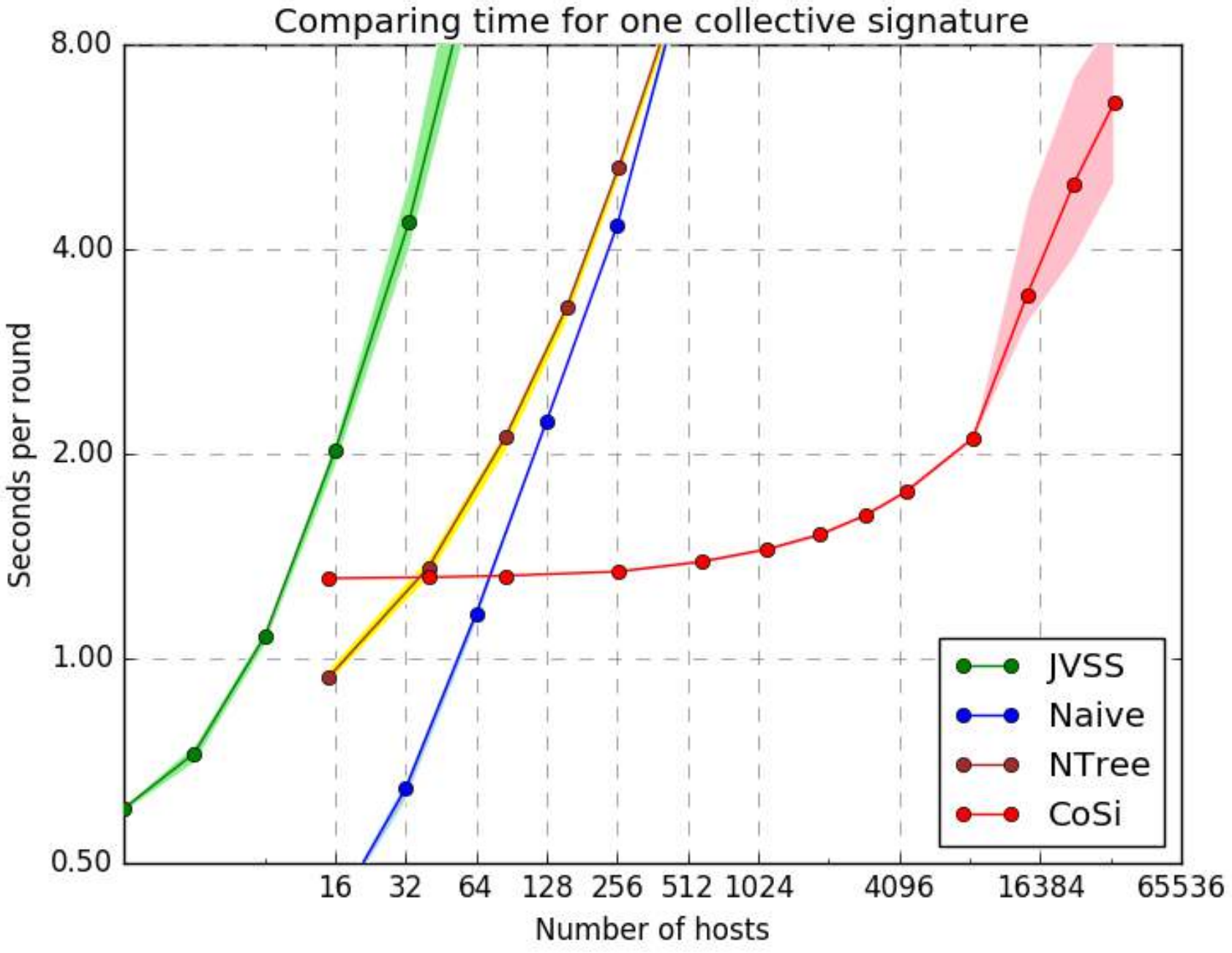
- Responses r_i
- Aggregate responses $\underline{r}_i$

Each $(c,\underline{r}_i)$ forms valid **partial** signature

$(c,\underline{r}_1)$ forms **complete** signature

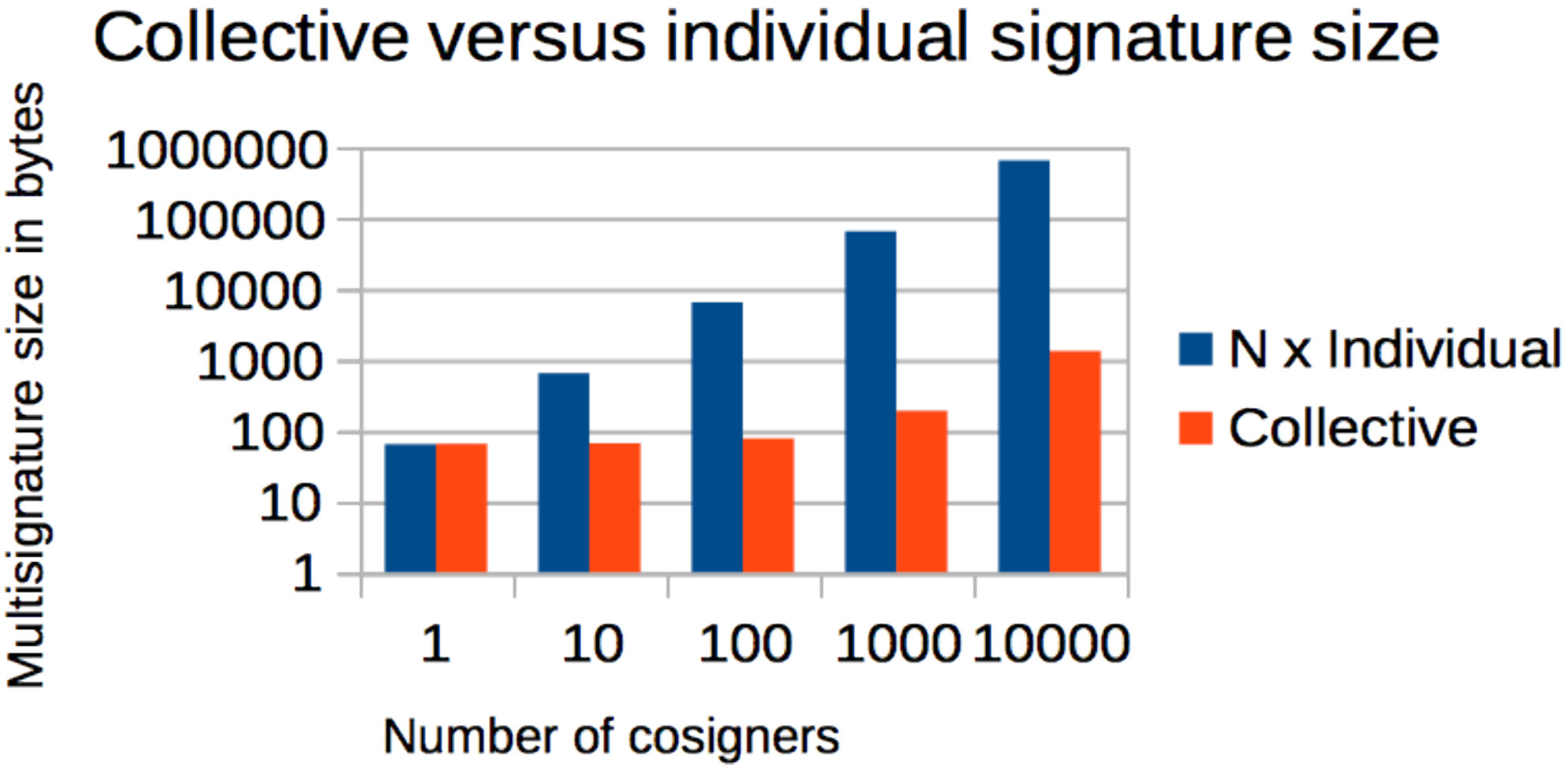


Results: Collective Signing Time

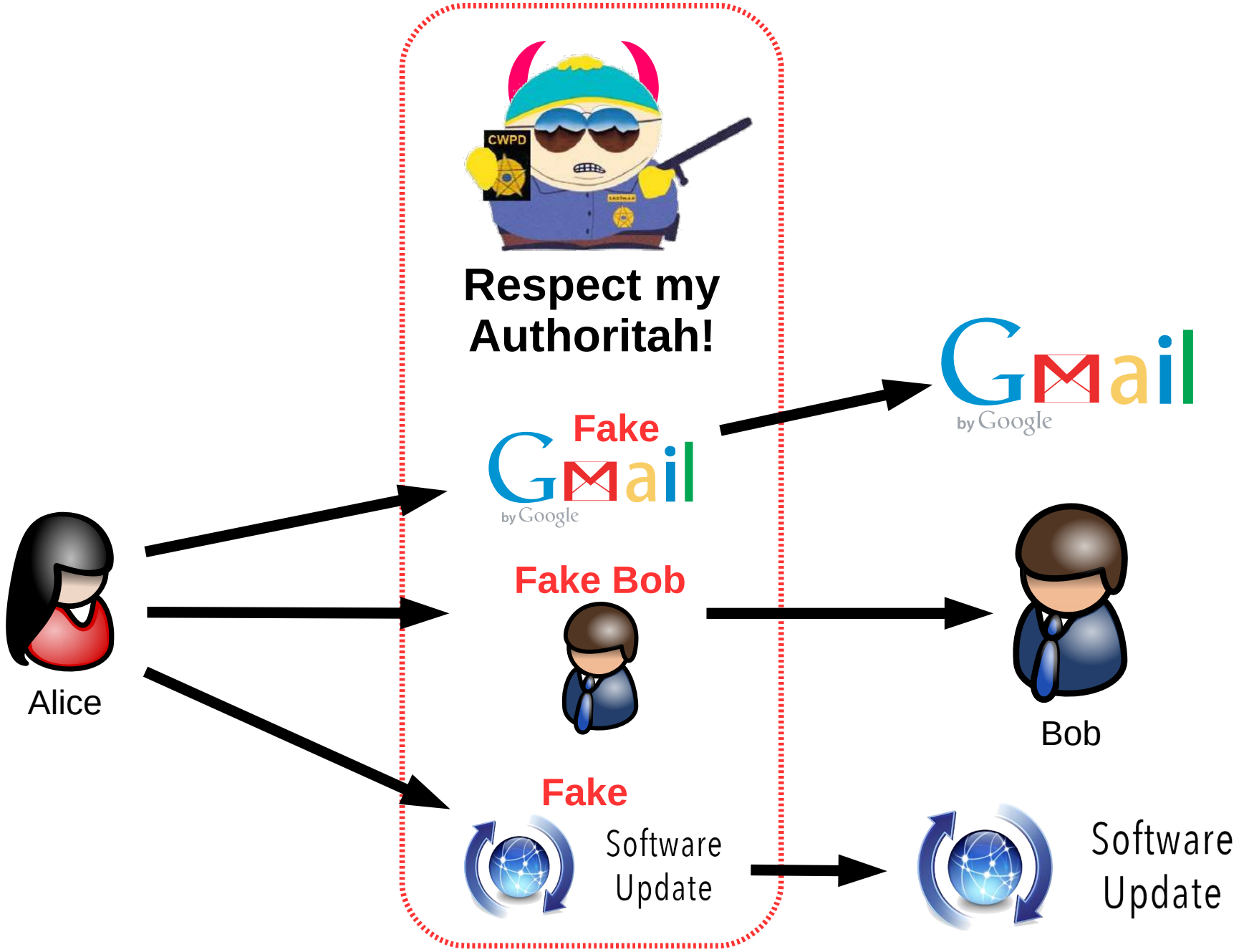


Results: Collective Signature Size

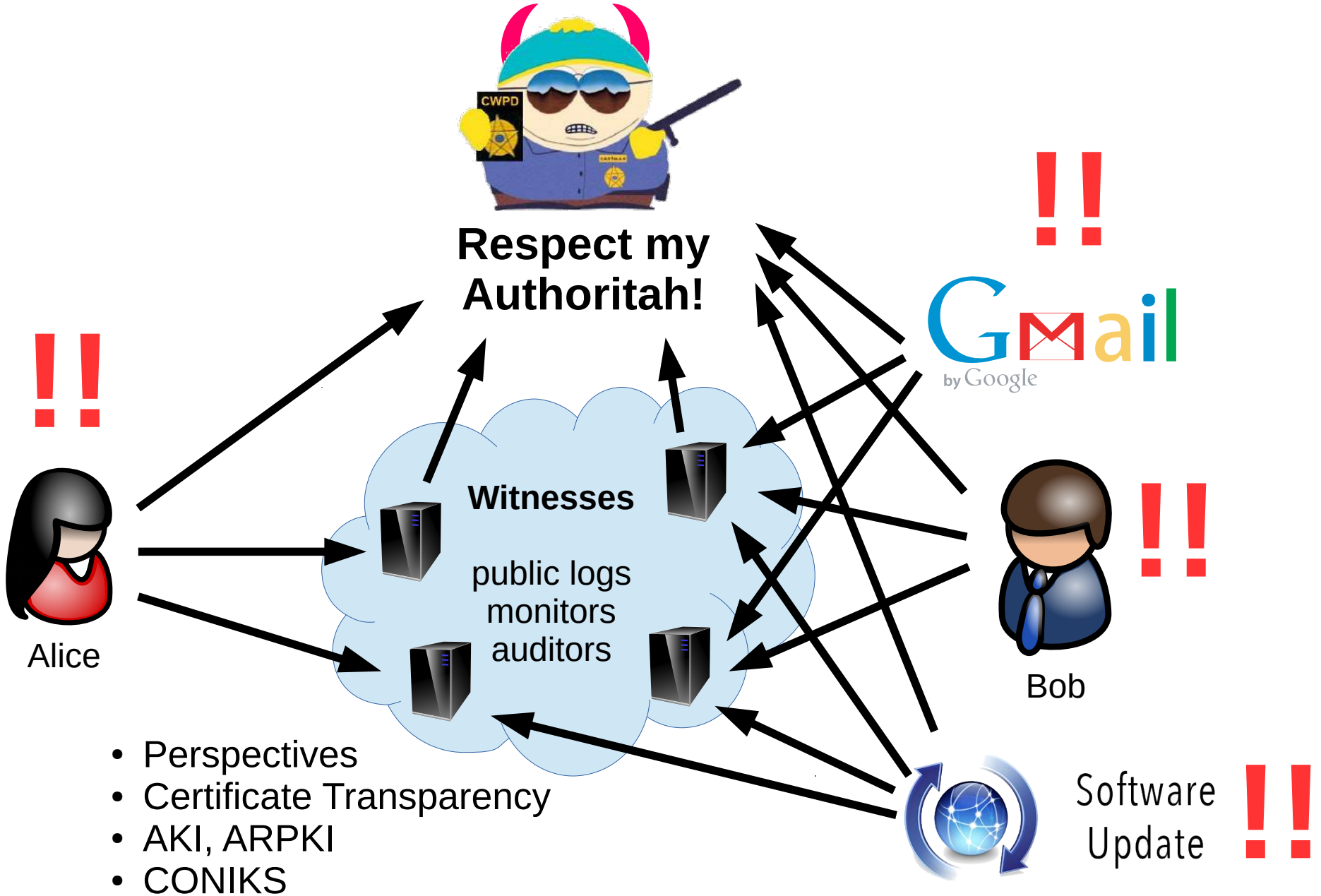
Ed25519: up to 512x smaller than N signatures



The Transparency Challenge



Existing Transparency Solutions



- Perspectives
- Certificate Transparency
- AKI, ARPKI
- CONIKS

A Real Scenario: Apple vs FBI

FBI: *"Sign an iOS with a backdoor."* Apple: *"No."*

Public debate **this time**,
but what about next time?

Will we **know** if a software
vendor is secretly coerced
to sign backdoored image?

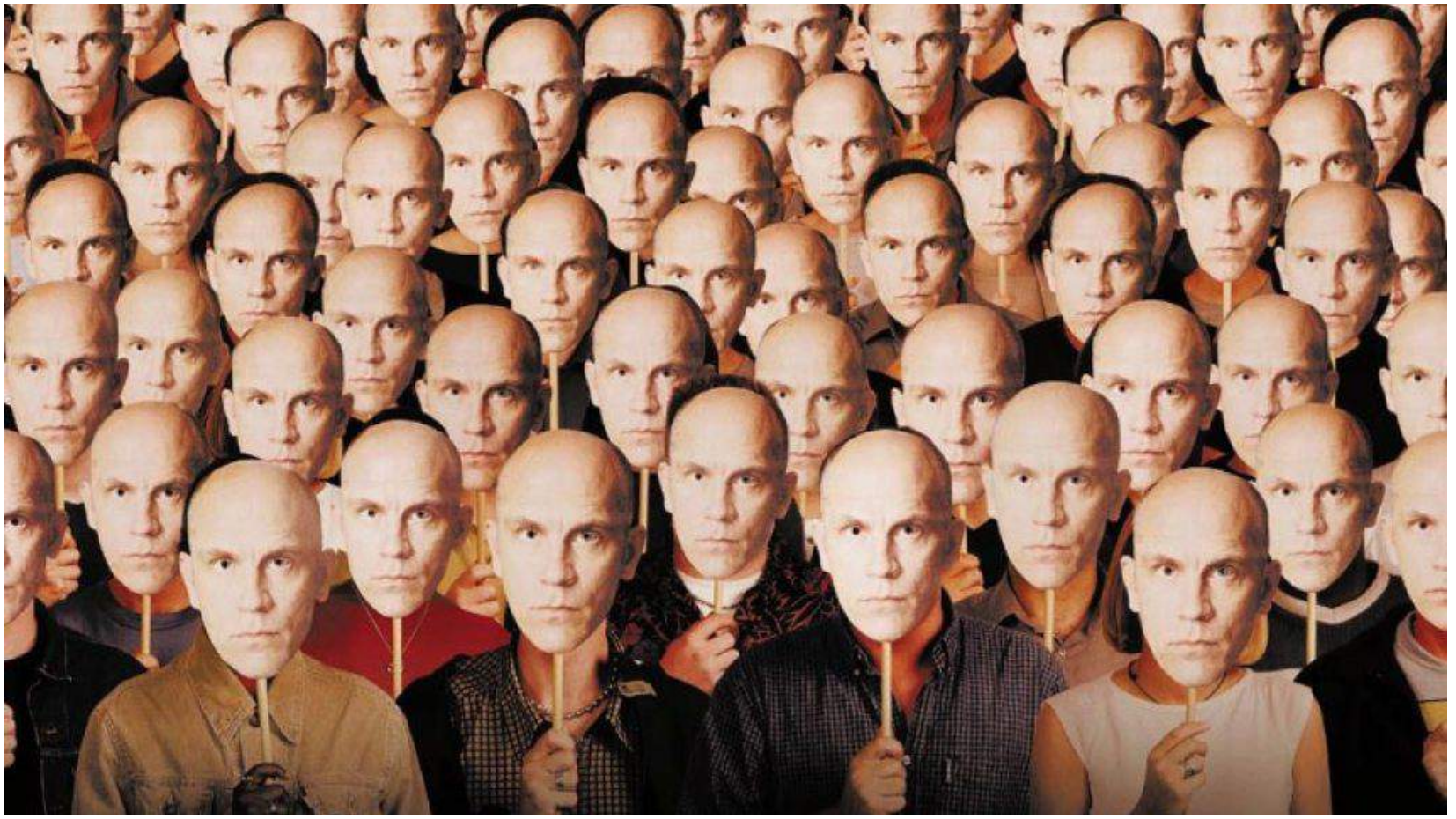
- A phone **sealed in a forensics lab** can't gossip!

Only collective signing can ensure transparency
even if attacked device is isolated

- **"Apple, FBI, and Software Transparency"**
  (Princeton "Freedom to Tinker" blog)

How to form witness groups?

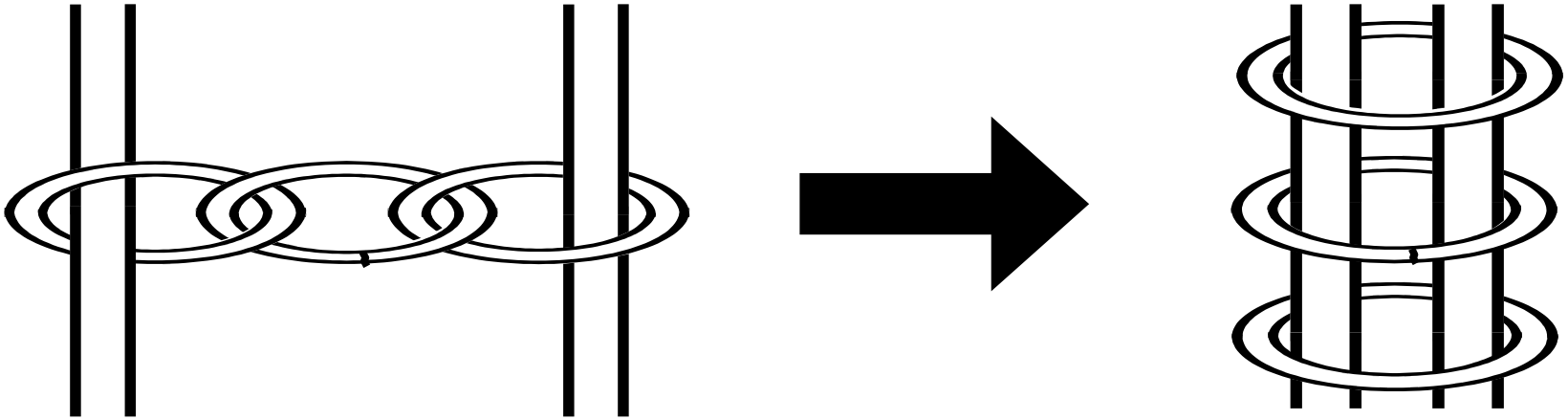
Leaving group “open to all” is insecure:
must be public list, selected to “make sense”



The “fake people” problem bites again

Talk Outline

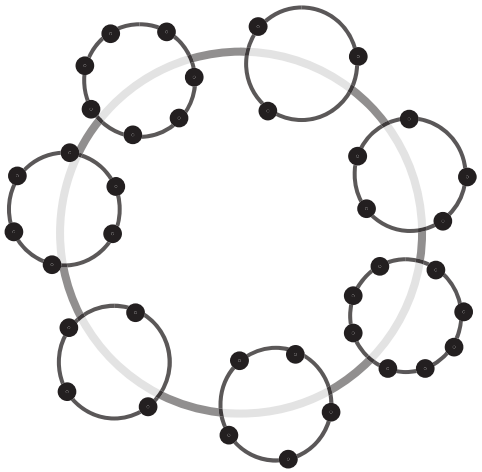
- Lessons from building decentralized anonymity systems
- The need for decentralized authorities
- Baby step: decentralized witness cosigning with CoSi
- **Baby step: decentralized public randomness**
- Next step: scalable consistent blockchains with ByzCoin
- Conclusion: can decentralization survive the fake people?



Unbiased Public Randomness

Need authority that can “flip coins” in public, convince everyone result is **fair** and **unbiased**.

- Choose a lottery winner fairly
- Sample ballots in election auditing
- Pick BFT clusters from large pool of servers
- Divide large user network into smaller random representative sets
  - e.g., for anonymity as in Herbivore [Goel/Sirer '04]
  - e.g., for scalable “sharded” blockchains



Random Related Randomness

Some existing approaches:

- Random oracles: Cachin et al, PODC 2000
- Quorum-building: King et al, ICDCN 2011
- Slow hashes: Lenstra/Wesolowski, 2015
- Via blockchains: Bonneau et al, …

But can we preserve simple “threshold model”, make it scale?

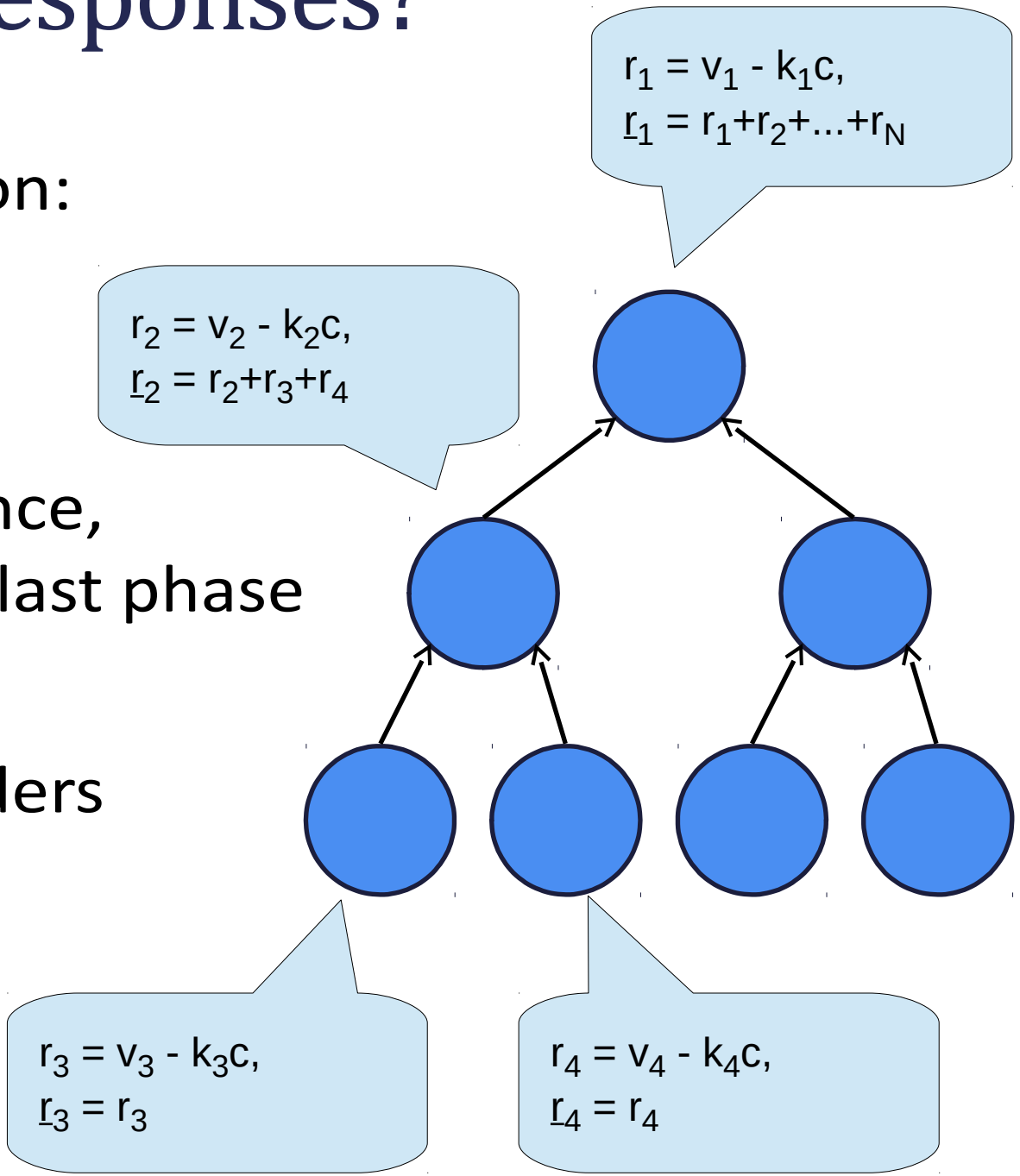
CoSi Protocol Responses?

Appealing near-solution:

- Contributions from all participants
- Committed in advance, unpredictable until last phase

But can still be *biased* by leader with *k* colluders

- Use exceptions to pick "best of" 2^k outcomes



Public Randomness: The Caveat

Current version with exceptions for availability:

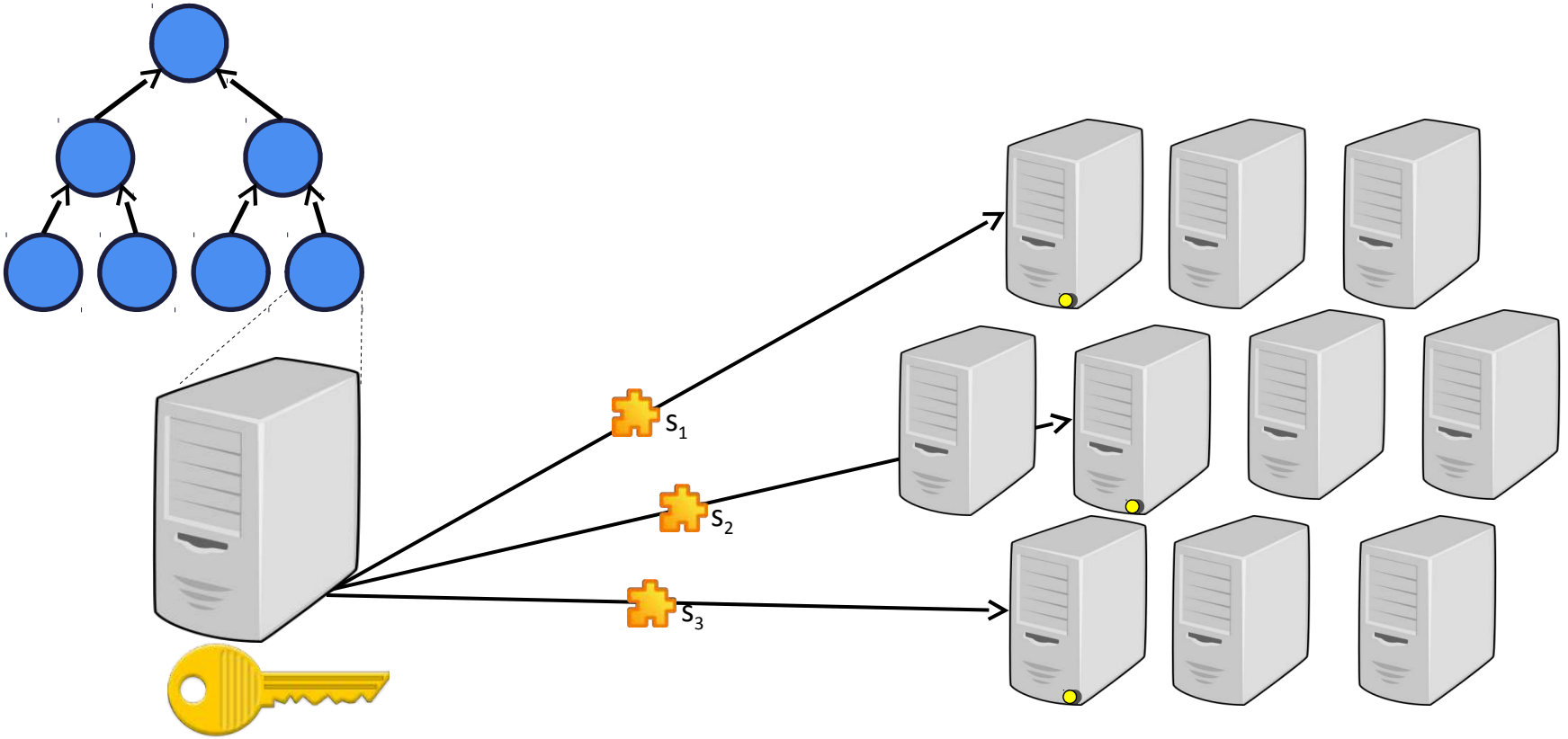
- Protects from anyone **predicting the future**
- Protects from anyone **rigging the outcome**
- ***Not*** fully **bias-protected** if leader is malicious

Attack: assume leader colludes with k followers

- Followers pretend to be offline in 2^k configs
- Leader picks “best” of 2^k possible outcomes

Availability via “life insurance”

- Node "insures" its private key by depositing the key shares with threshold group of “trustee” servers
  - Shamir verifiable secret sharing (VSS)
- Trustees can sign on behalf of failed node



The Challenge

How to pick set of trustees for given witness?

- All nodes trustees (JVSS): doesn't scale, O(N^2)
- Witness-chosen: can pick bad group → DoS
- Leader-chosen: pick cronies, get secret early

We need **unbiased public randomness**
to pick these random trustee subgroups,
to get **unbiased public randomness!**

→ **“**randomness bootstrap” protocol

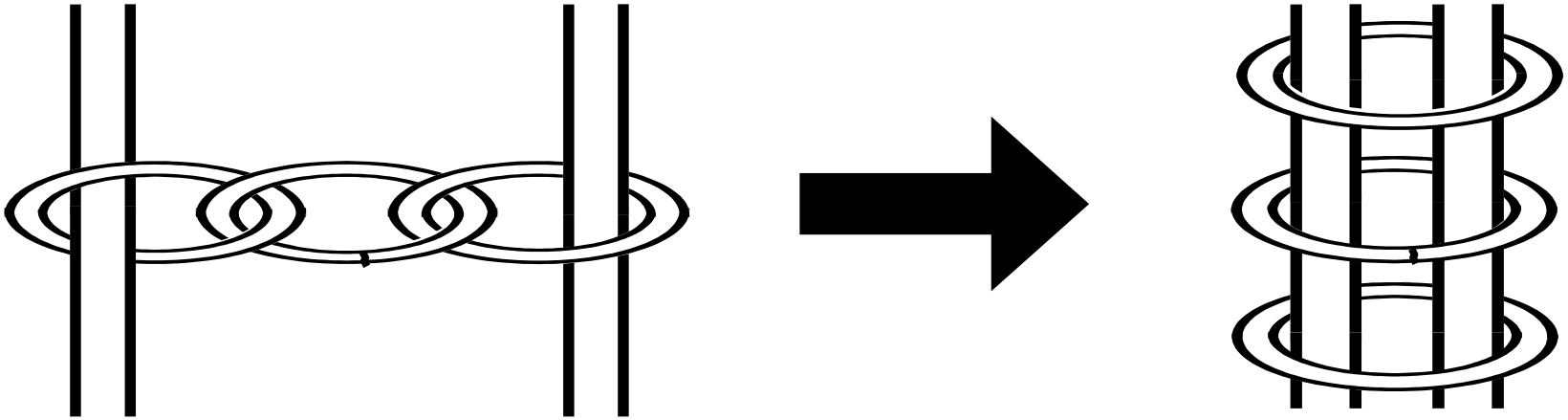
RandHound: Protocol Sketch

Intuition: bootstrap from
pairwise unbiased randomness

1) Leader commits to random value R_L,
   each follower *i* commits to random R_i
2) Reveal; follower *i* picks trustees via H(R_L,R_i),
   deals secret S_i to picked trustees
3) Leader commits to threshold set of secrets
   s.t. must include *at least one* honest follower
4) Followers reveal dealt secret shares

Talk Outline

- Lessons from building decentralized anonymity systems
- The need for decentralized authorities
- Baby step: decentralized witness cosigning with CoSi
- Baby step: decentralized public randomness
- **Next step: scalable consistent blockchains with ByzCoin**
- Conclusion: can decentralization survive the fake people?



The Call of the Blockchain

(credit: Tony Arcieri)

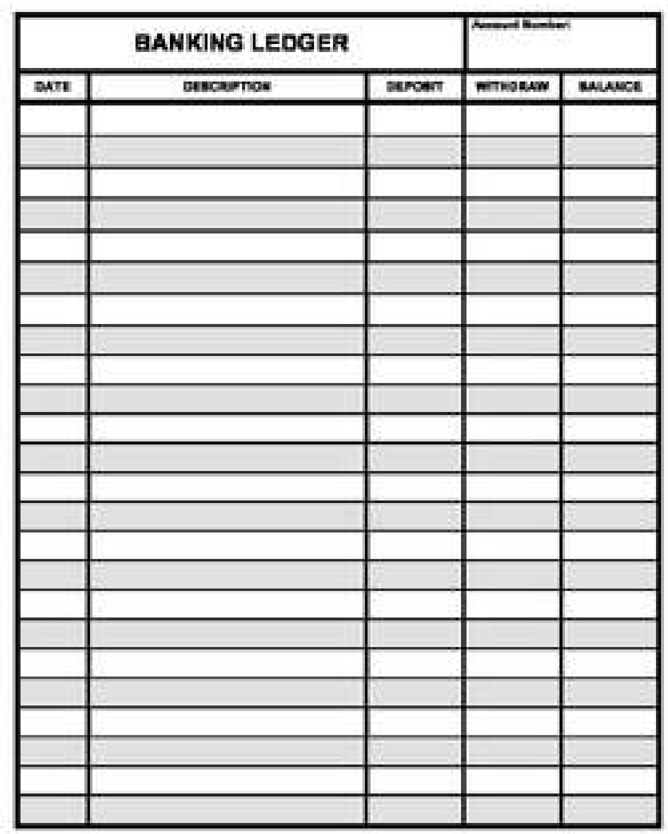
Basic Foundations for Money

Things

- Gold, beads, cash...

Ledgers

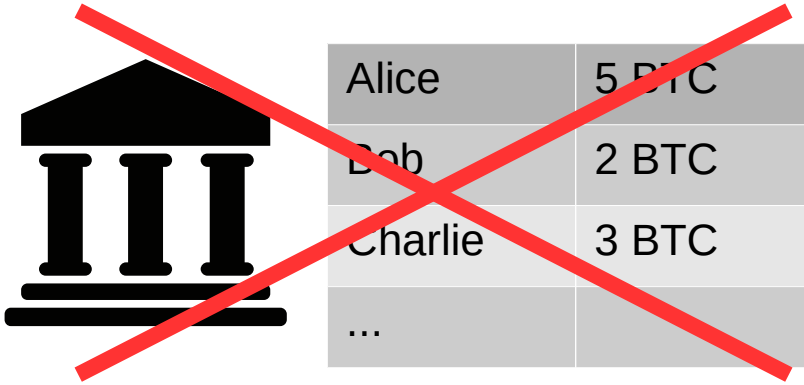
- Who owns what?



BANKING LEDGER				Account Number:
DATE	DESCRIPTION	DEPOSIT	WITHDRAW	BALANCE

Decentralized Public Ledgers

Problem: we don't want to trust any designated, centralized authority to maintain the ledger



Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Solution: "everyone" keeps a copy of the ledger!

- Everyone checks everyone else's changes to it

Alice's copy

Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Bob's copy

Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Charlie's copy

Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

The Call of the Blockchain

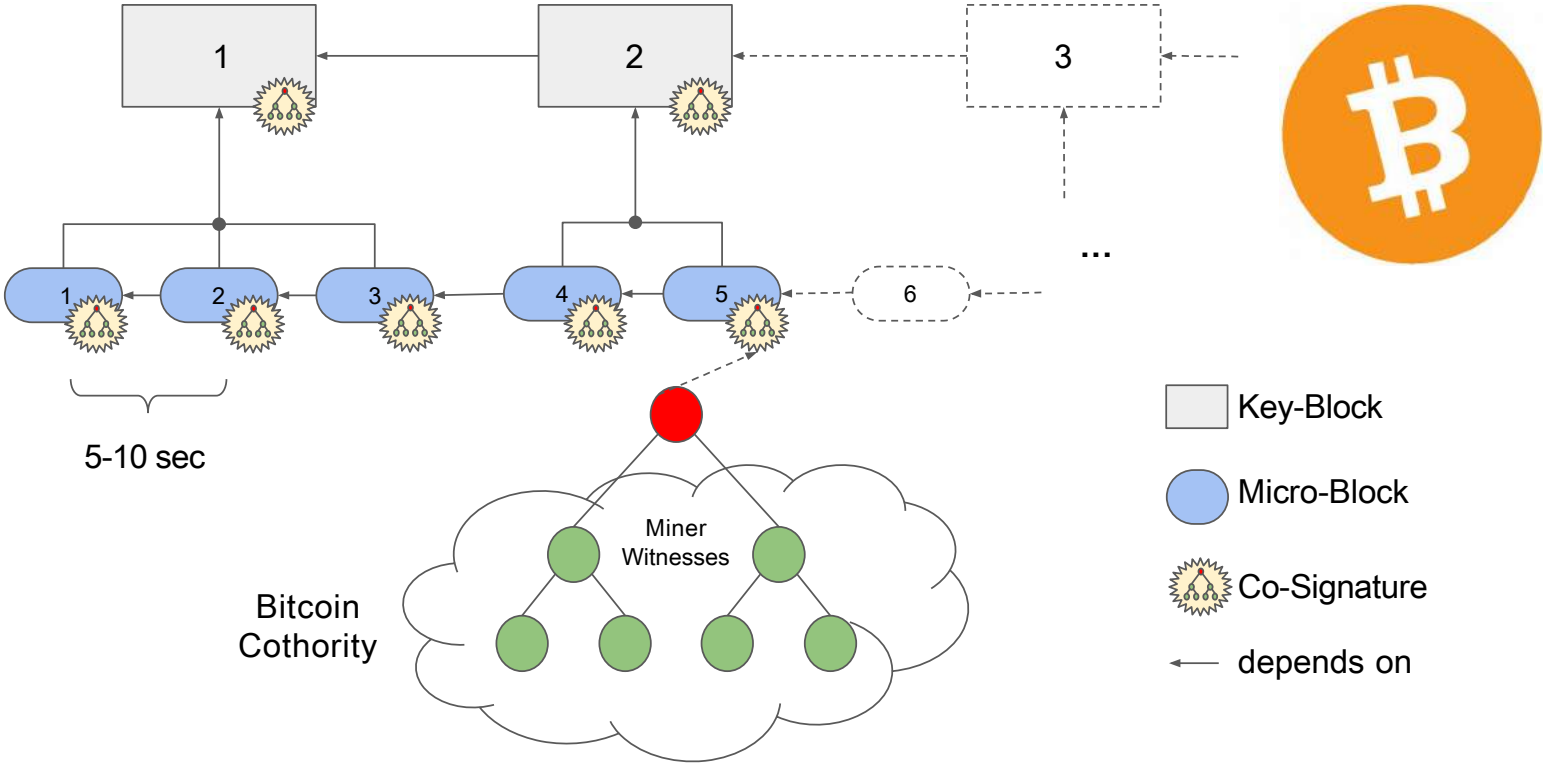
Decentralized ledgers: powerful idea

- But huge scalability, security challenges

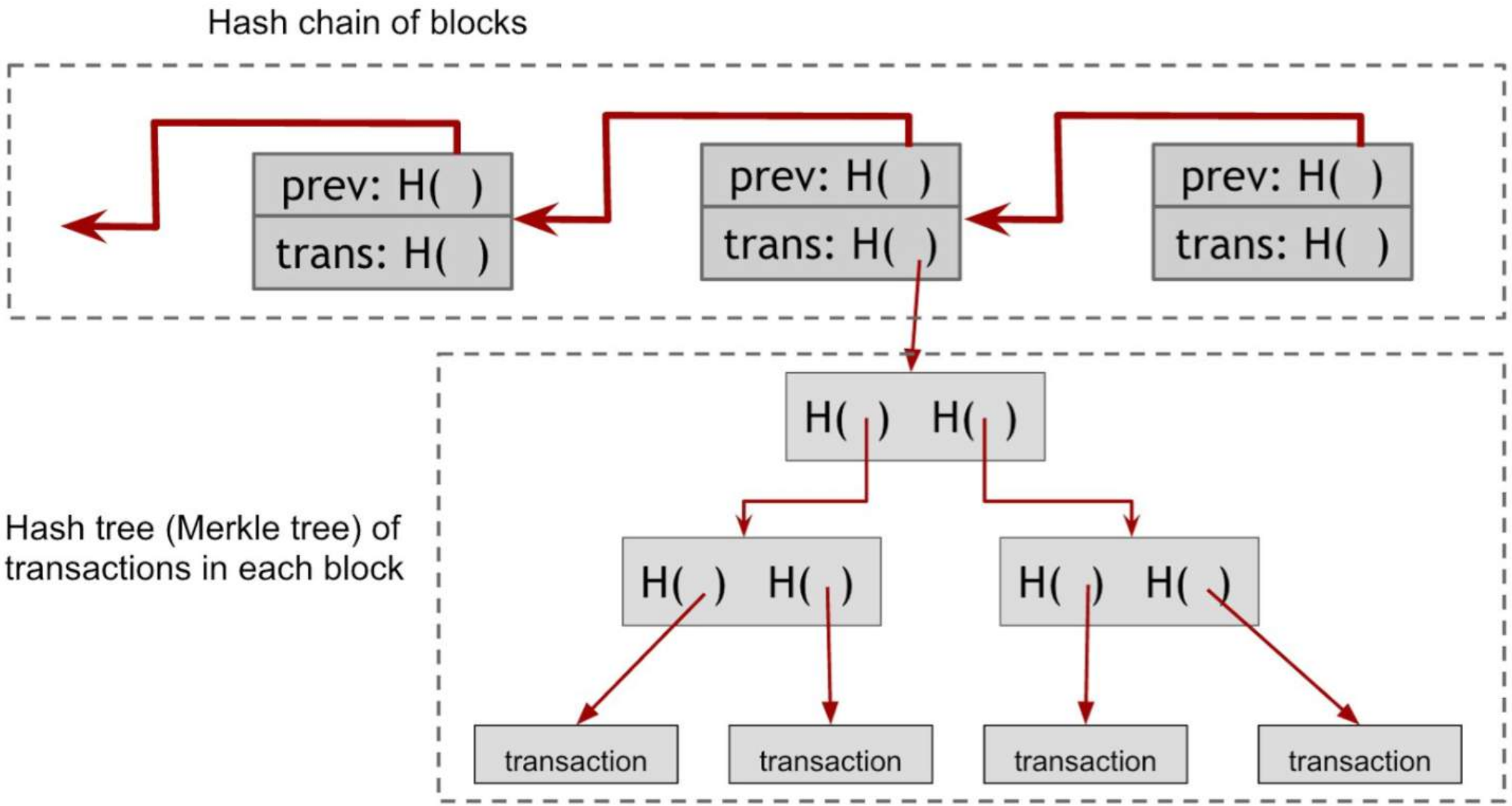
Scaling Blockchains with ByzCoin

"Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing"

- To appear at USENIX Security 2016
- Draft: http://arxiv.org/abs/1602.06997



The Bitcoin Blockchain



Key Bitcoin Challenges

Ground-breaking, exciting, but…

1. Guarantees only **probabilistic** consensus
2. Takes **10mins or 1hr** to commit transaction
3. Limited to about **7 transaction/second**
4. Full nodes **store** whole blockchain “forever”
5. Proof-of-work **mining** is huge energy waste

ByzCoin addresses #1-3, a bit #4, **not** #5

Decentralized Consensus

Who decides **what changes to make** to log?

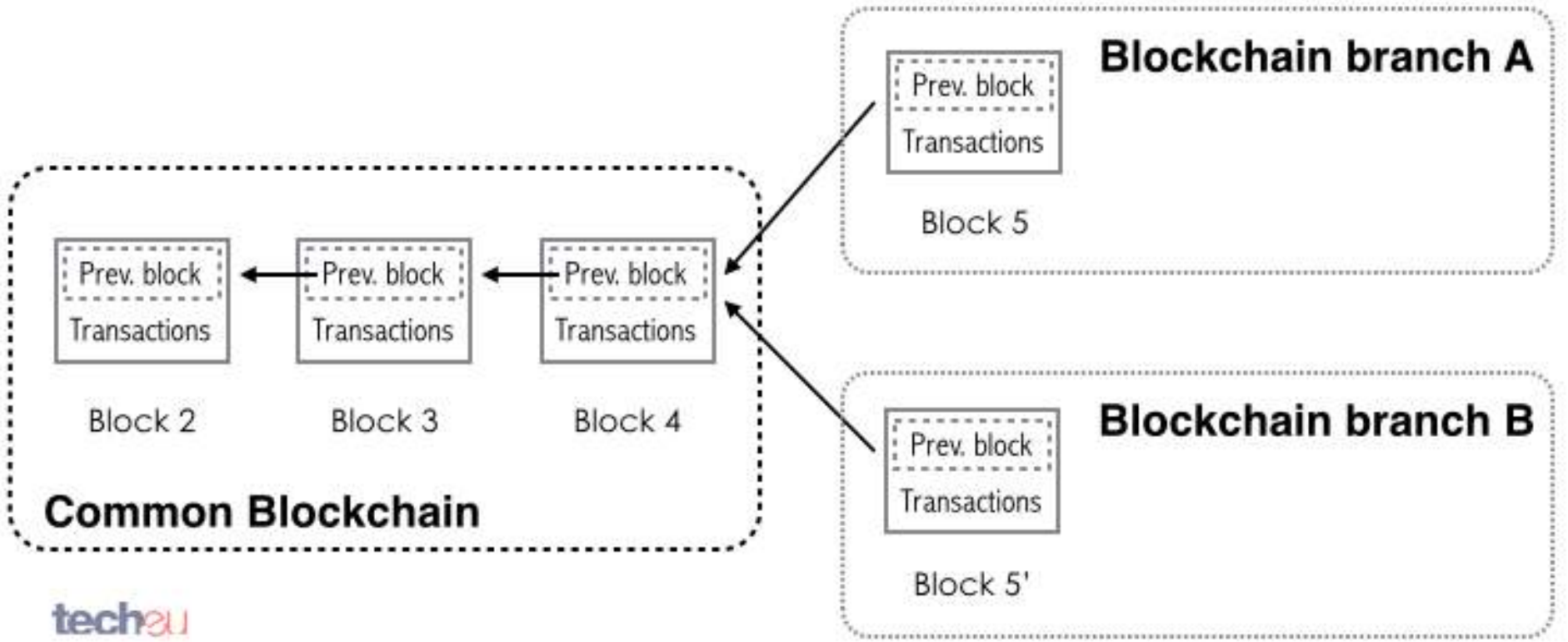
Bitcoin miners who process transactions

- Each miner “plays a lottery” constantly, gets series of randomly-numbered “tickets”
- Each ticket has small probability of “winning”
- Each successive lottery winner earns the right to append **one new block** to the blockchain
  - One block may contain **many transactions**
- By design, one lottery winner every ~10mins

Bitcoin consensus is probabilistic

If two miners win at **about the same time,**

the blockchain **forks**:

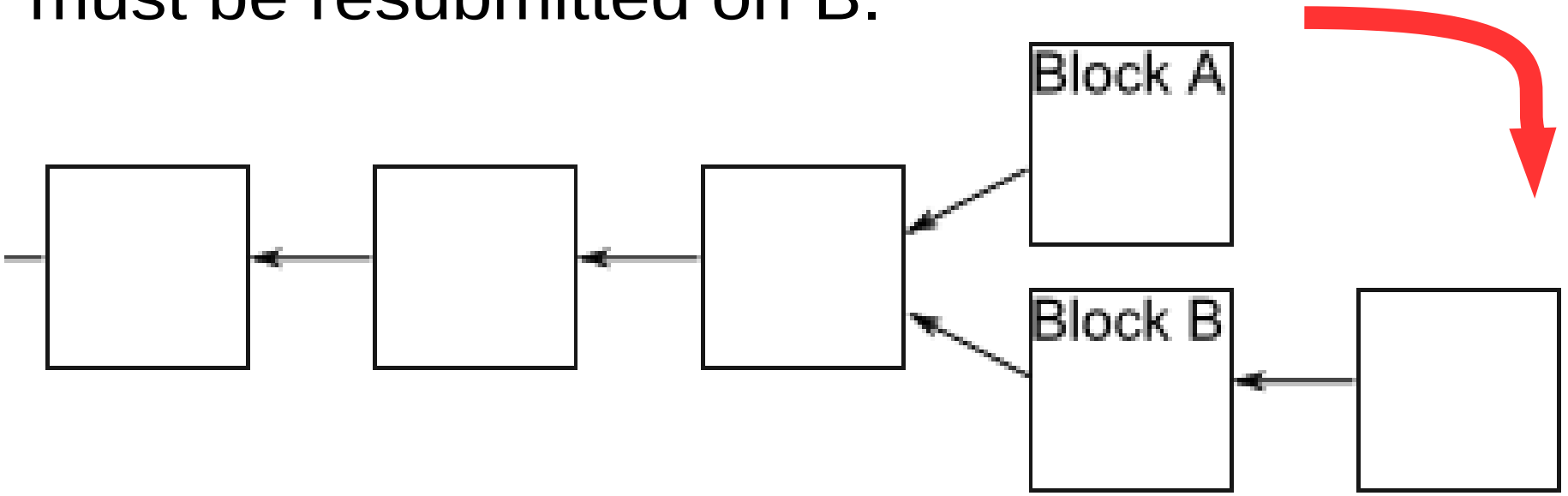


Resolving Temporary Forks

Example:

As soon as miner “wins” a ticket to extend B, miners on A “jump ship” to B's history.

- Any transactions only appearing in block A will “disappear from history,” must be resubmitted on B.



Byzantine Consensus

PBFT: “Practical Byzantine Fault Tolerance”

- Castro/Liskov ‘99 – landmark paper
- Large body of follow-on work

Assumes n-member **consensus group**

Ensures **strict serialization** of transactions

- Provided <1/3 of group is faulty: n >= 3f + 1

In practice assumes **fixed group, small n**

Why is PBFT in Bitcoin “hard”?

1) **PBFT** assumes closed consensus group,

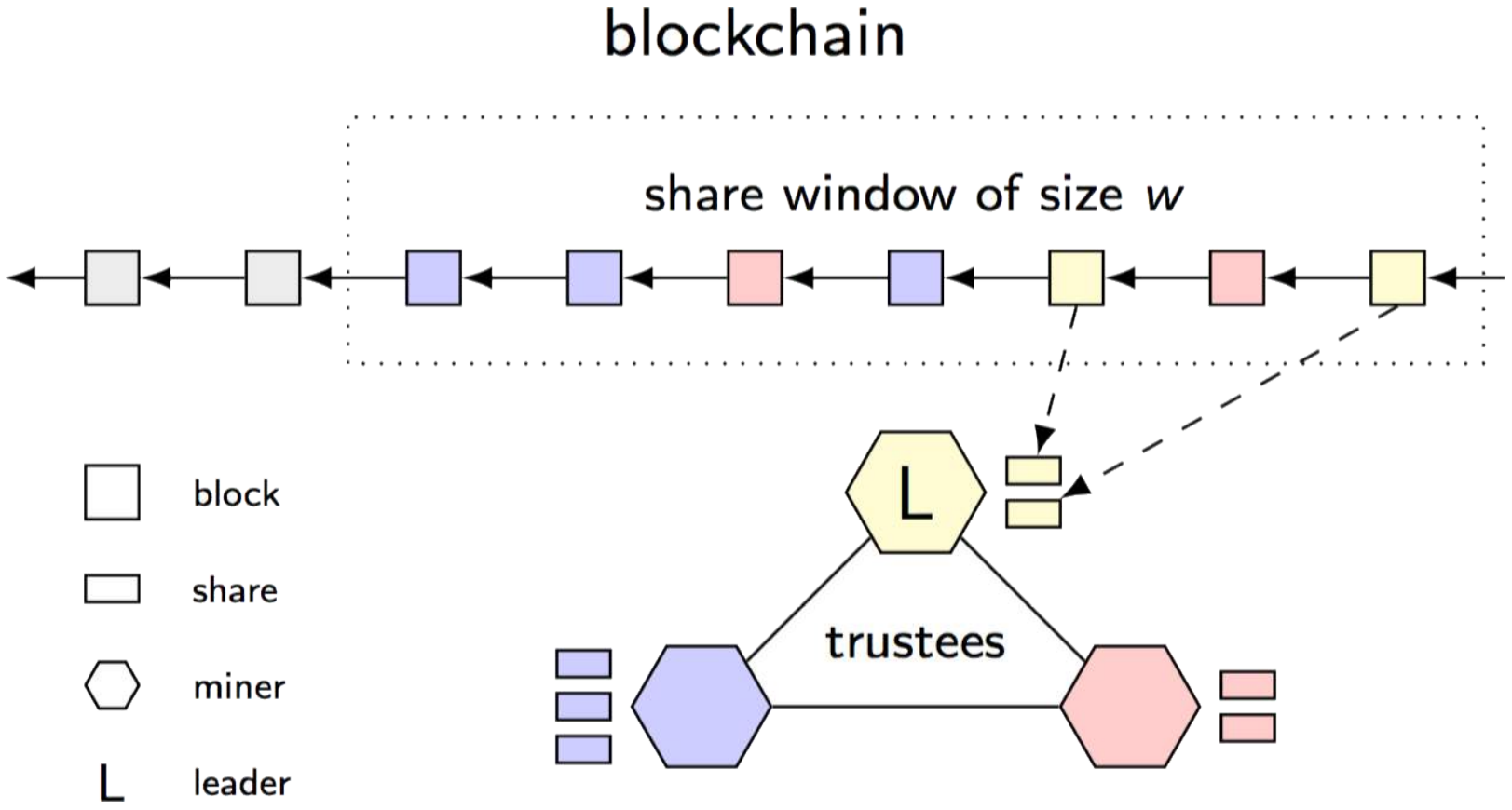
   Bitcoin mining is “open to all” (kinda)

2) **PBFT** implementations assume small **n**
   (typically n=4, never more than ~15);

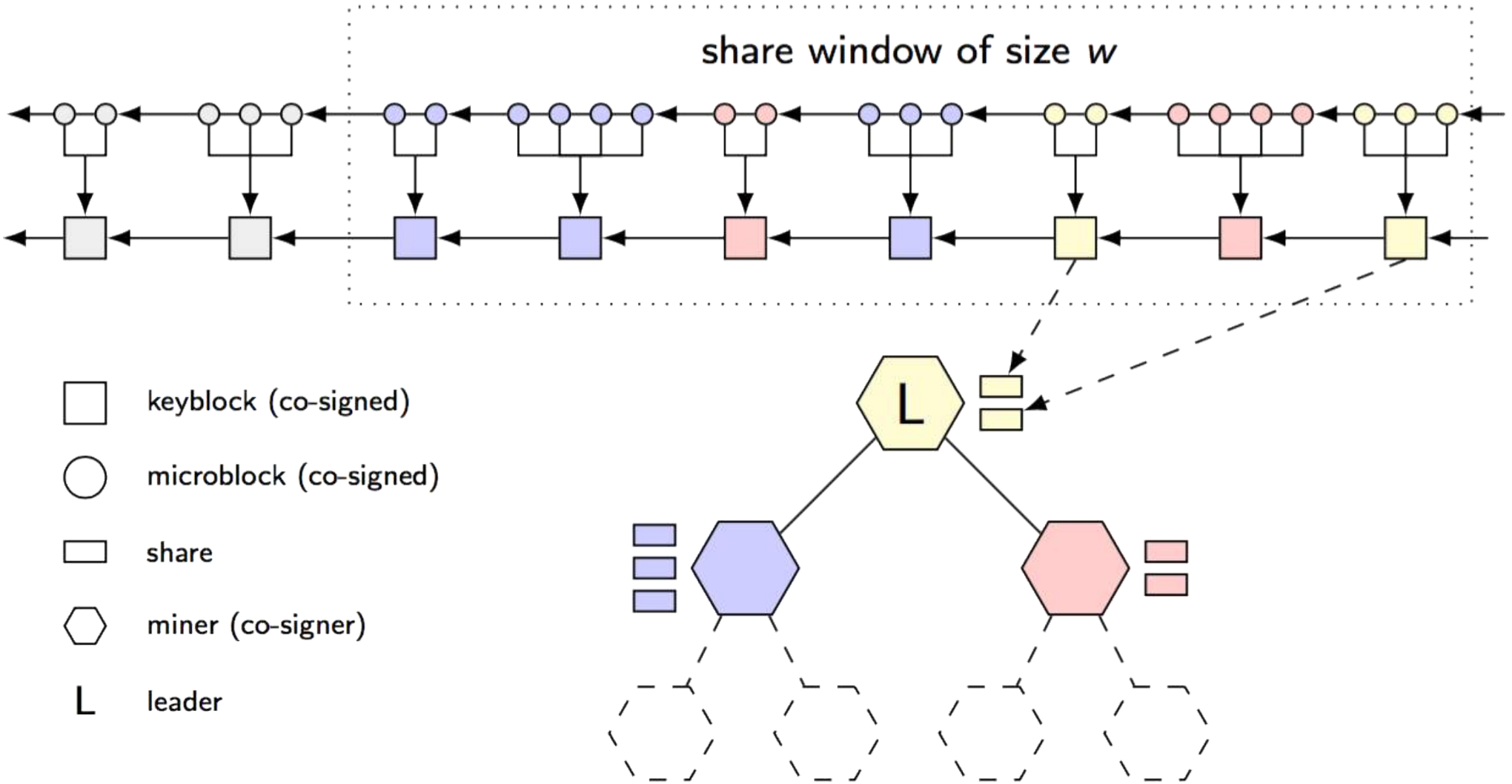
   Bitcoin has many miners
   (1000s, maybe 100k)

ByzCoin Consensus Windows

Keeps Bitcoin's proof-of-work (PoW), but mining yields **temporary membership share** in a gradually-rotating consensus group



Decoupled mining in ByzCoin

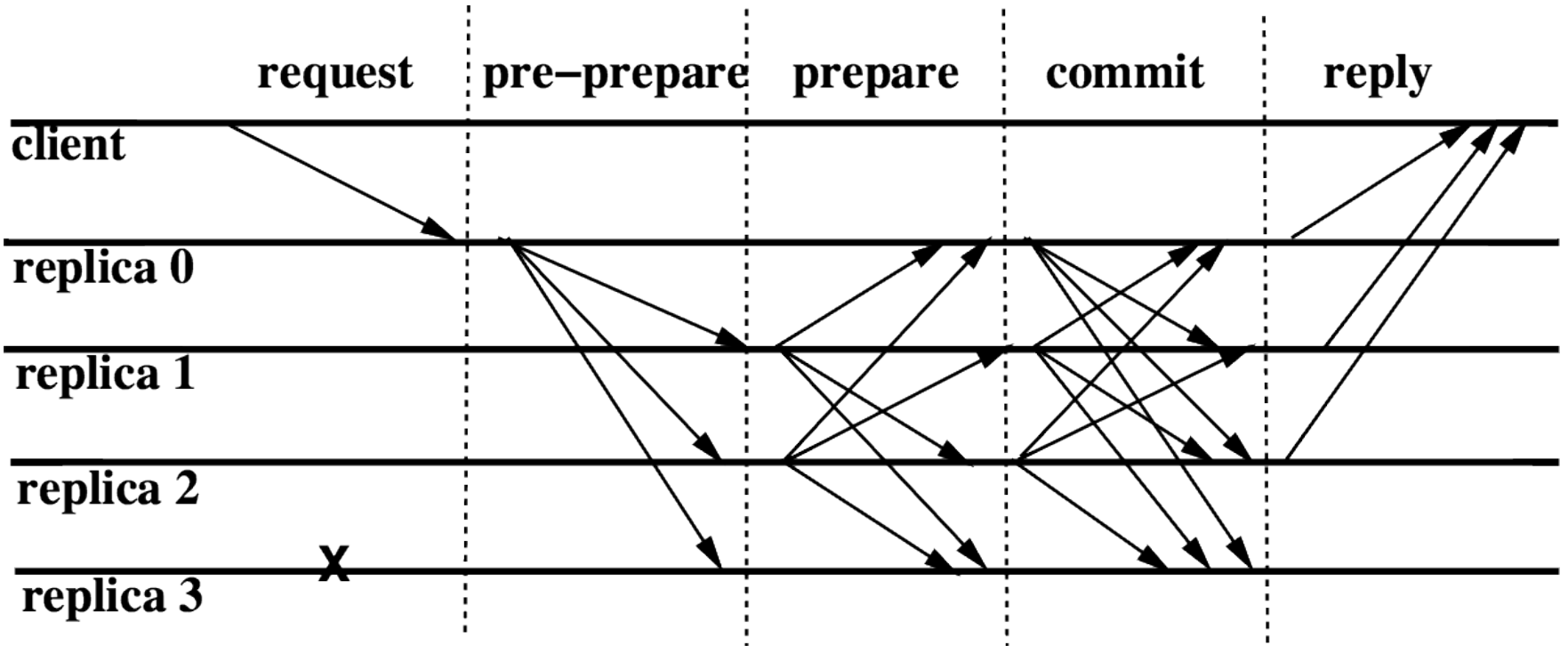


PBFT Scalability

Three phase: pre-prepare, prepare, commit

In prepare & commit, leader must get at least two-thirds of all participants to “sign-off”

- Nodes sign-off via broadcast: $O(N^2)$

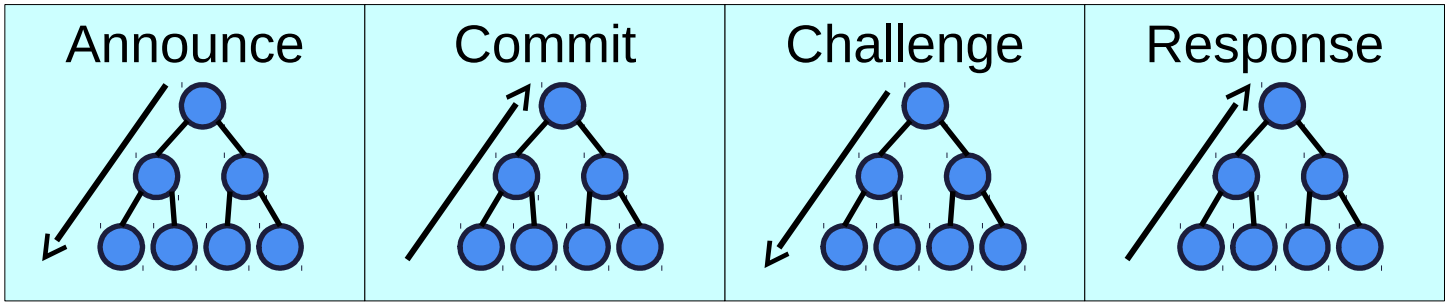


PBFT with Collective Signing

ByzCoin runs **collective signing** rounds
to implement PBFT prepare, commit phases

- Efficient tree-structured communication
- Sign-offs compressed into 1 signature

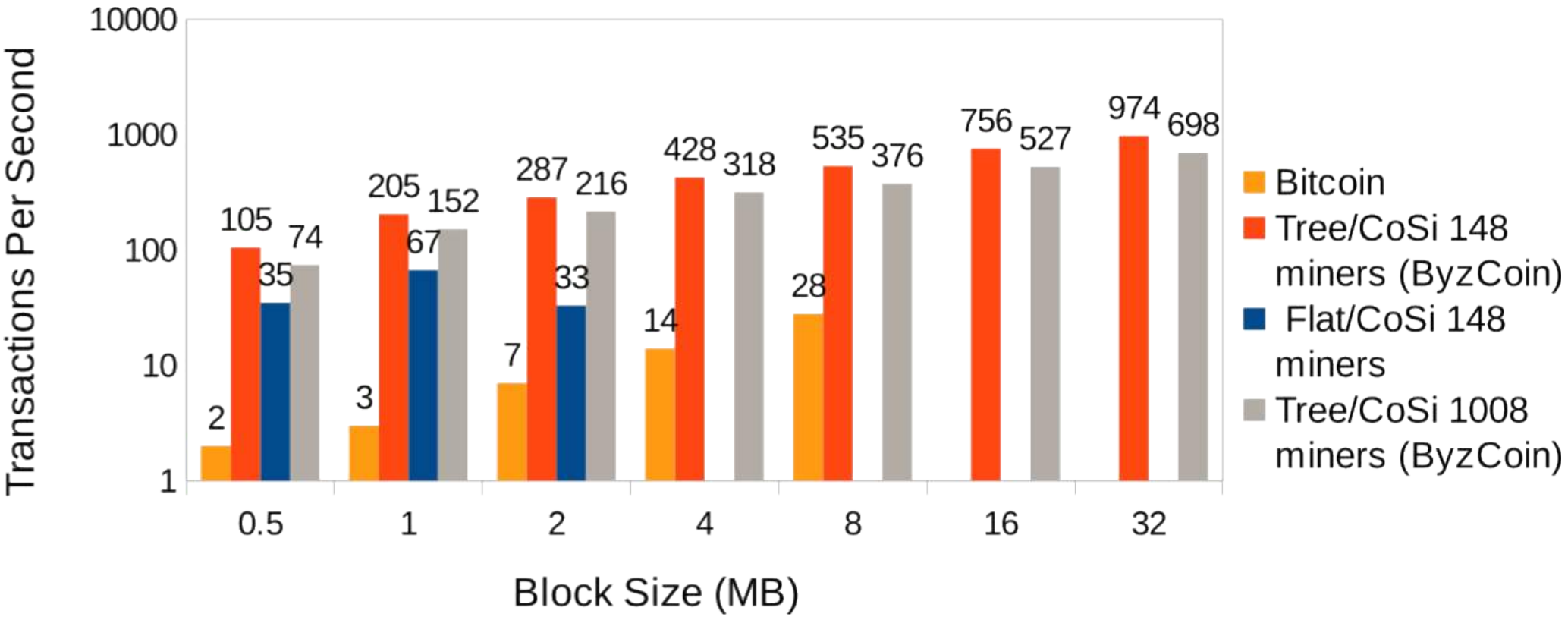
Reduce round cost from $O(N^2)$ to ~$O(N)$



ByzCoin transaction throughput

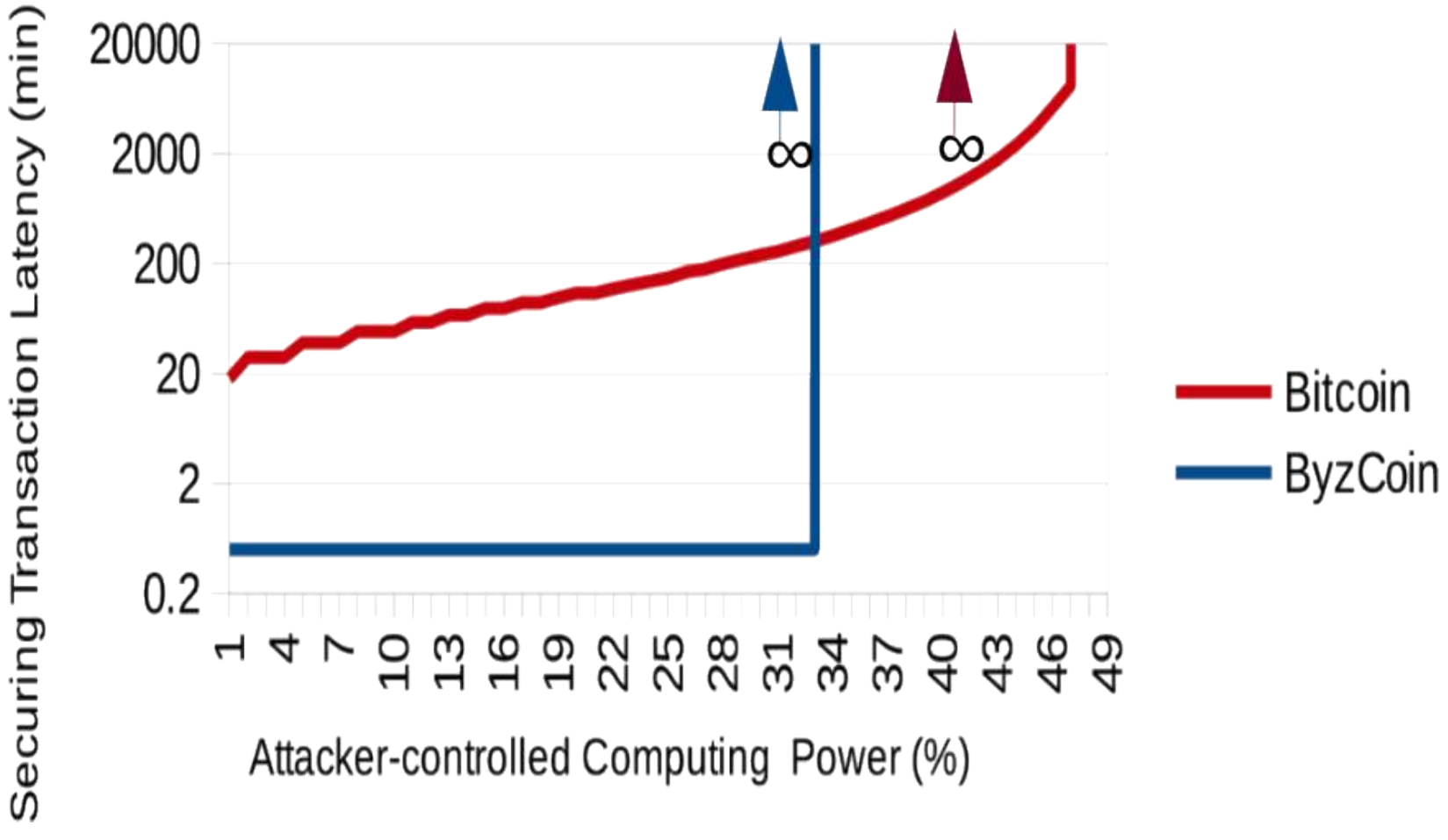
~100x improvement for similar block size

- higher throughput than PayPal



ByzCoin Consistency

ByzCoin transactions become irrevocable immediately upon PBFT commitment

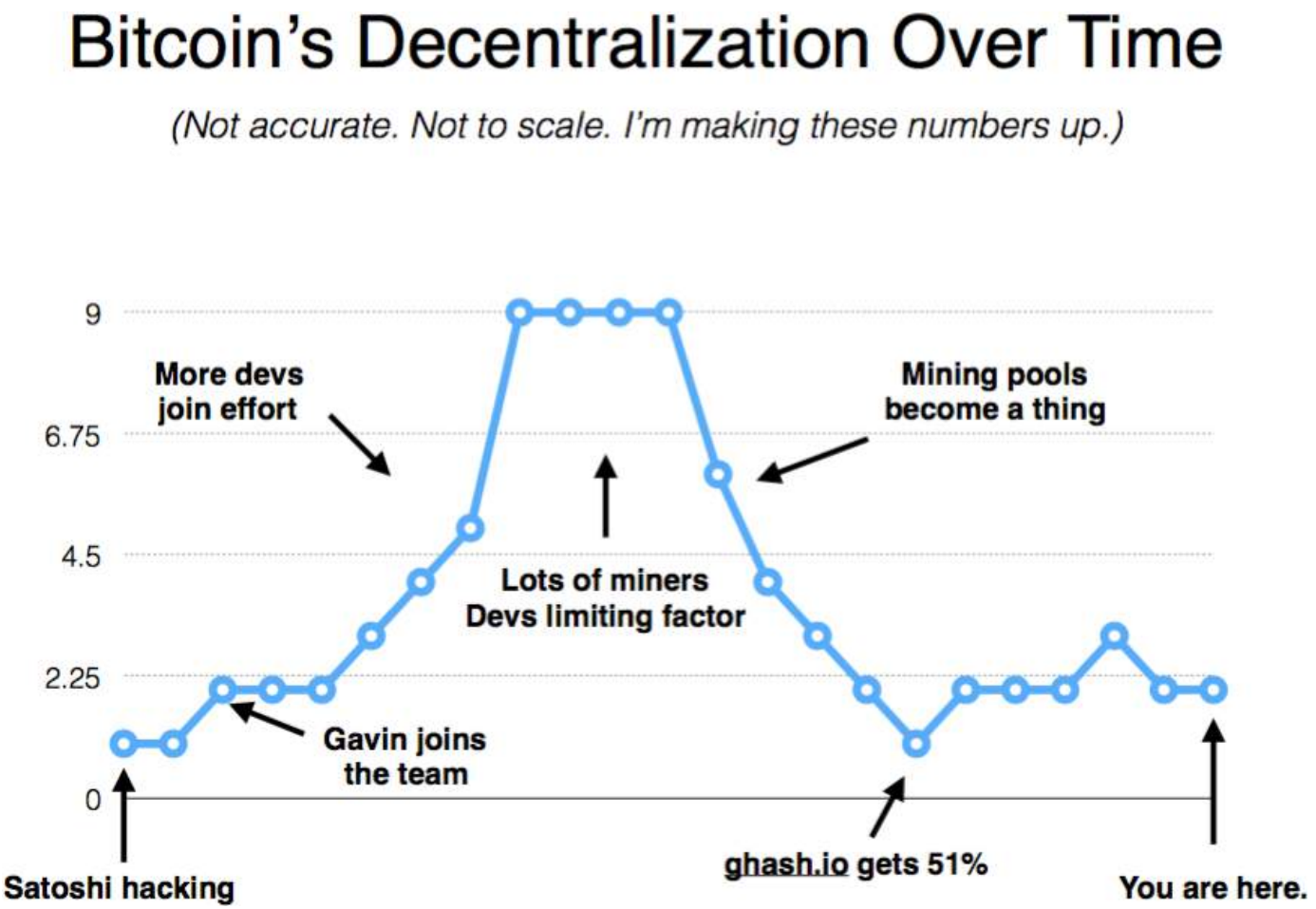


Limitations

- Prototype, experiments still preliminary
- Doesn’t address downsides of PoW
- Like PBFT, assumes synchronous network
- Like PBFT, may have subtle DoS and performance-downgrade attacks
- …

Conspicuously Unsolved: Mining

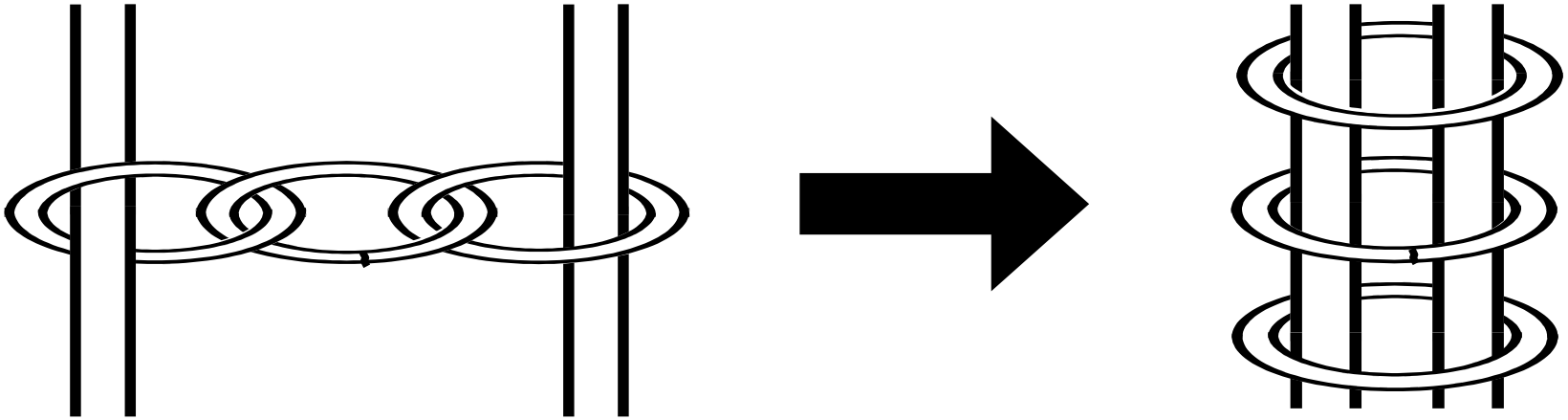
...a **horrible** solution to the Sybil attack



Credit: Greg Slepak, "Deconfusing Decentralization"

Talk Outline

- Lessons from building decentralized anonymity systems
- The need for decentralized authorities
- Baby step: decentralized witness cosigning with CoSi
- Baby step: decentralized public randomness
- Next step: scalable consistent blockchains with ByzCoin
- **Conclusion: can decentralization survive the fake people?**



Two Key Challenges for Decentralized Systems, Revisited

How can we make decentralized systems

1) Scalable enough to empower **all the people?**
2) Empower only **real people, not fake people?**

We're getting a handle on #1, what about #2?

- Killed USENET, killing Tor, killing Bitcoin?
- Proposition: there is no "**pure tech**" solution

Contrast: a 2003 "Anon-Optimist" Perspective…

Queers Anonymous: Lesbians, Gay Men, Free Speech, and Cyberspace

---

Edward Stein[*]

Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society.[1]

Pseudonymity allows people who are experimenting with different sorts of interests to do so without social repercussions. People can temporarily obscure their real life and play with a different conception of what their life might be.[2]

…with a 2014 "Anon-Pessimist" Perspective

The New York Times

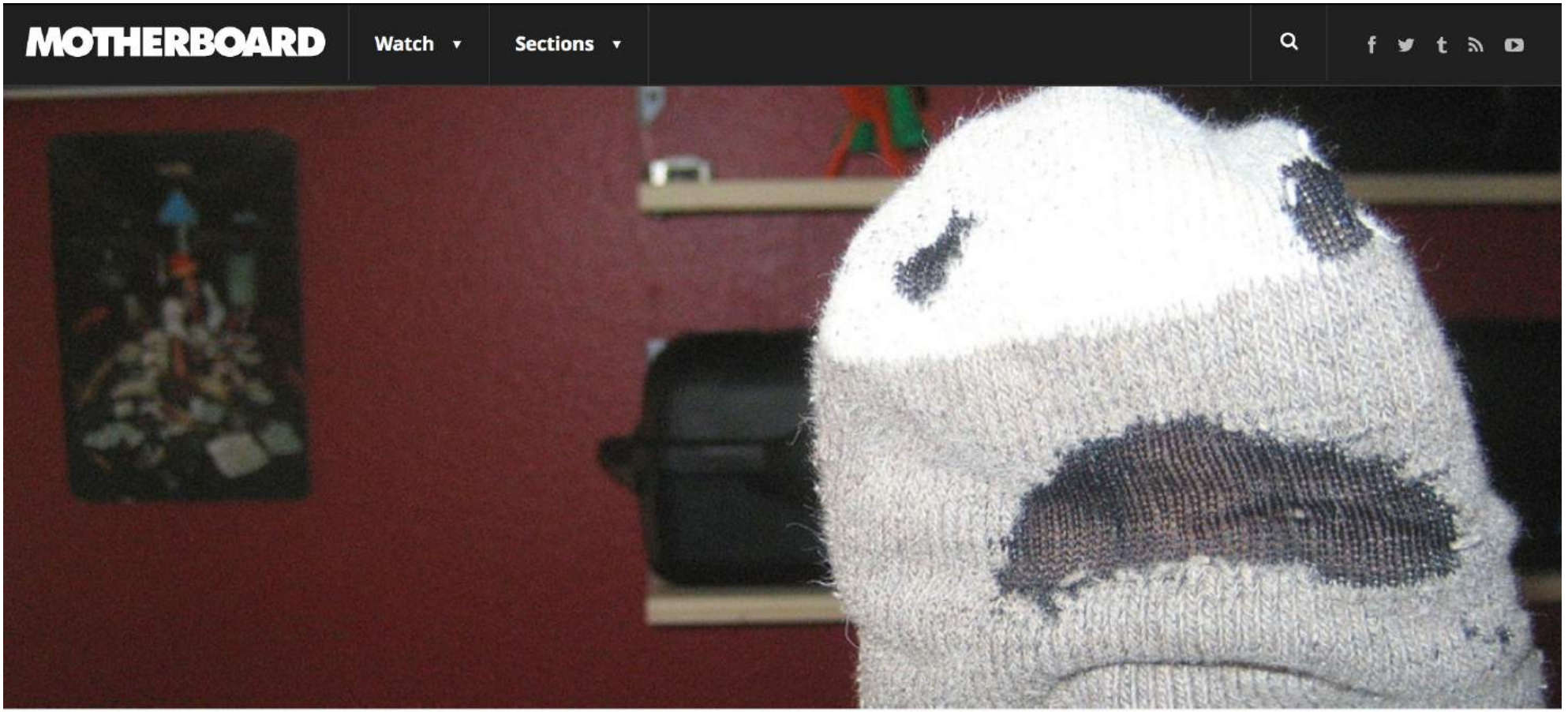
Women and Minorities as Targets of Attack Online

Kristy Tillman is the design director at Society of Grownups, where she is currently leading the design effort to democratize financial literacy. She is on Twitter.

AUGUST 19, 2014

Anonymity on the web plays a precarious role in the ways we interact with each other. Some interactions justify, and are even strengthened by, anonymity – but it often comes with a huge price tag for marginalized communities on the web, leaving women and people of color to pick up the tab.

Anonymous abuse can get so bad…



That Time a Tor Developer Doxxed a Troll

December 3, 2014 // 07:00 AM EST

Written by
FRUZSINA EÖRDÖGH
CONTRIBUTOR

We Need Zero-Knowledge "Proofs of Real-Personhood"

But must have a foundation in the real world!

- IP addrs, Proof-of-[Work,Storage,Stake,etc] are just different measures of legacy wealth/power
- We *could* build on government-issued IDs
  - But who wants to trust governments to get it right?
- We *could* build on social media, federated ID
  - Anonymized via, e.g., Crypto-Book [CODASPY '16]
  - Weak, but Sybil attack cost measurable and >0

Could a "personhood-proof" foundation depend on little or no government, commercial infrastructure?

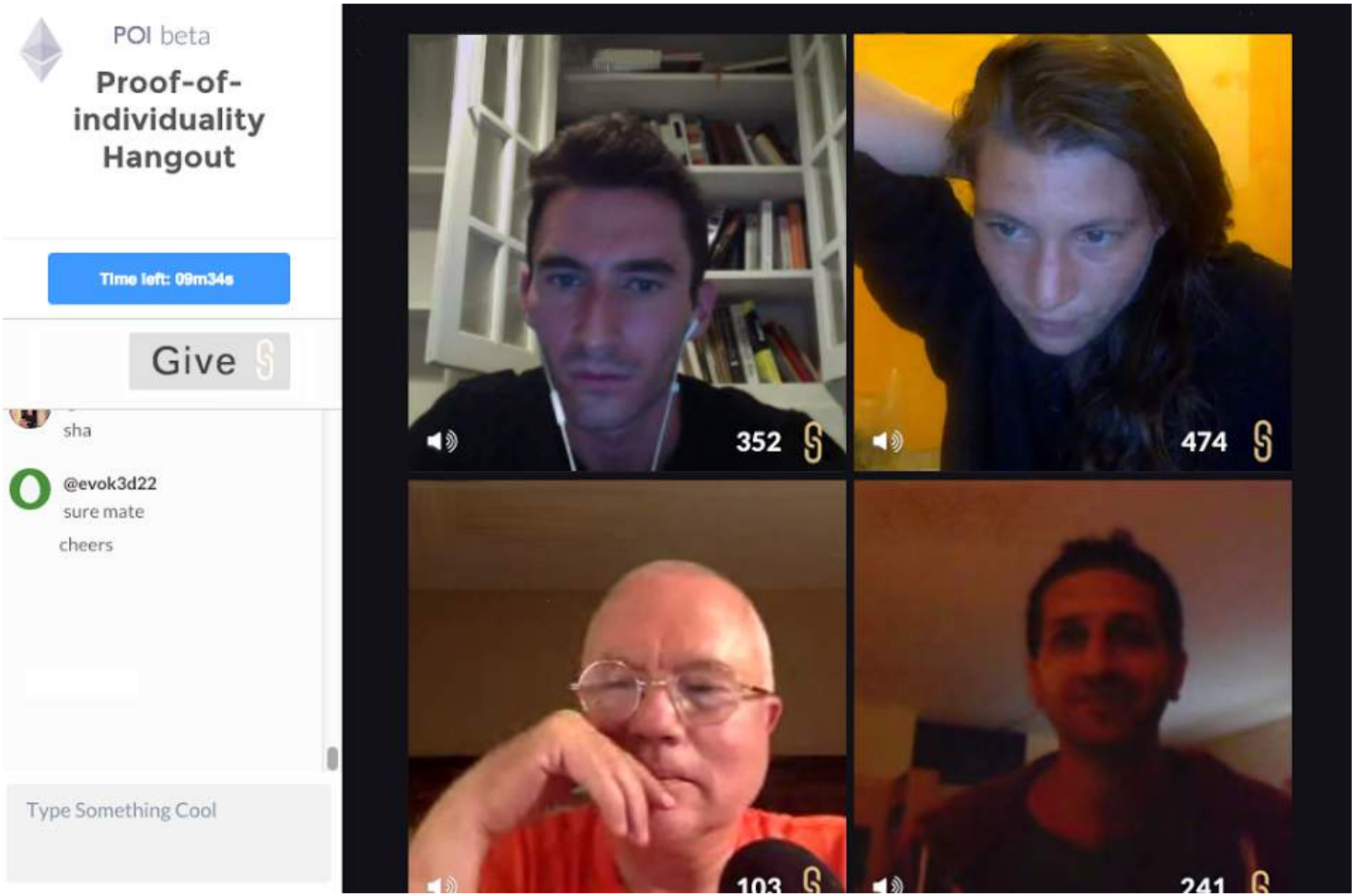
Need a physical-world solution

e.g., Pseudonym Parties [SocialNets ‘08]:

- One physical body → one pseudonym token

Need a physical-world solution

Or Proof-of-Individuality, an online equivalent?



The power of “real-person proofs”

Sybil-resistant reputation, moderation, anti-spam

- Could we eventually resurrect USENET?

Ad hoc anonymous polls, voting in open groups

- Bring “real democracy” to decentralized orgs

Crypto-currencies with “Floating Basic Income”?

- Each real person gets to mint 1 coin per month
- Open, permissionless, bottom-up: no government or industry investment required
- Value from scarcity, collective community trust

Time to stop building on quicksand

Perhaps the most urgently-needed
missing security foundation

may have no
purely technical solution

because it’s solvable only if
tied to real people

Conclusion

Secure decentralized (and centralized) systems increasingly need **decentralized authorities**

We've taken a few experimental baby steps…

- **AnonRep – anonymous reputation**
- **CoSi – decentralized witness cosigning**
- **ByzCoin – collectively signed blockchains**

But need to put together to build real systems…

And decentralized systems still lack a foundation for security allowing them to survive fake people

More details: https://github.com/dedis/cothority