Building Trust for Sample Voting

N.K.Blanchard

IRIF, RSVP, POPSpEC

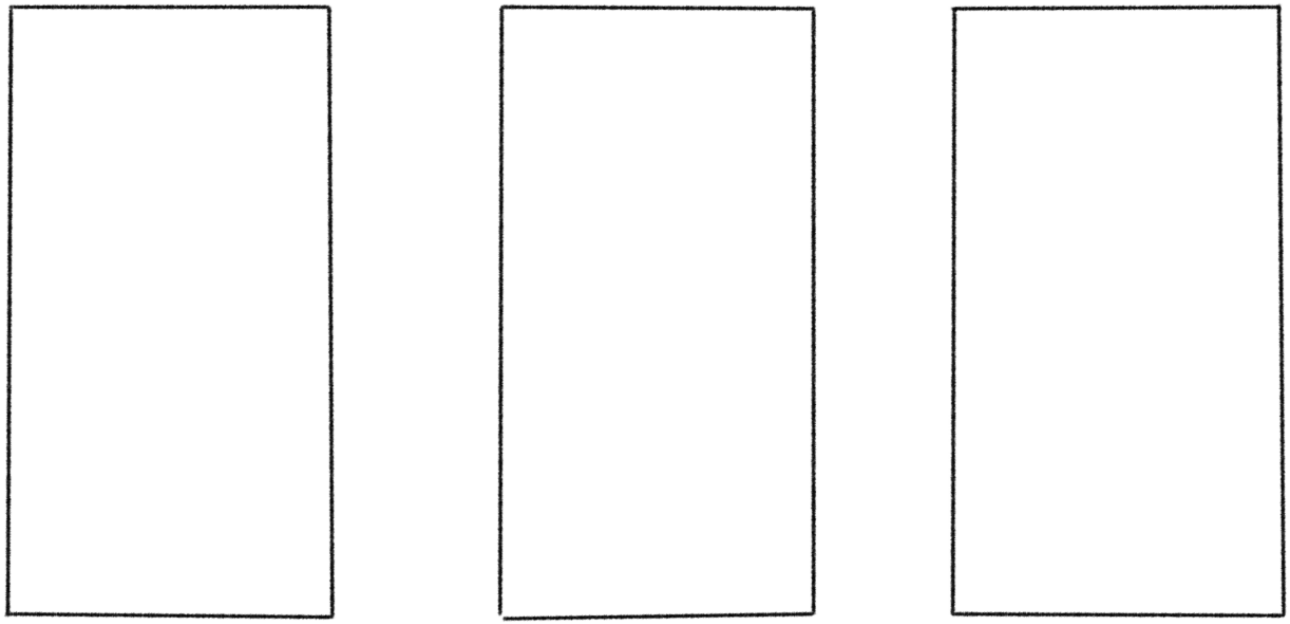
Talk at TeSS 2017

27th June 2017

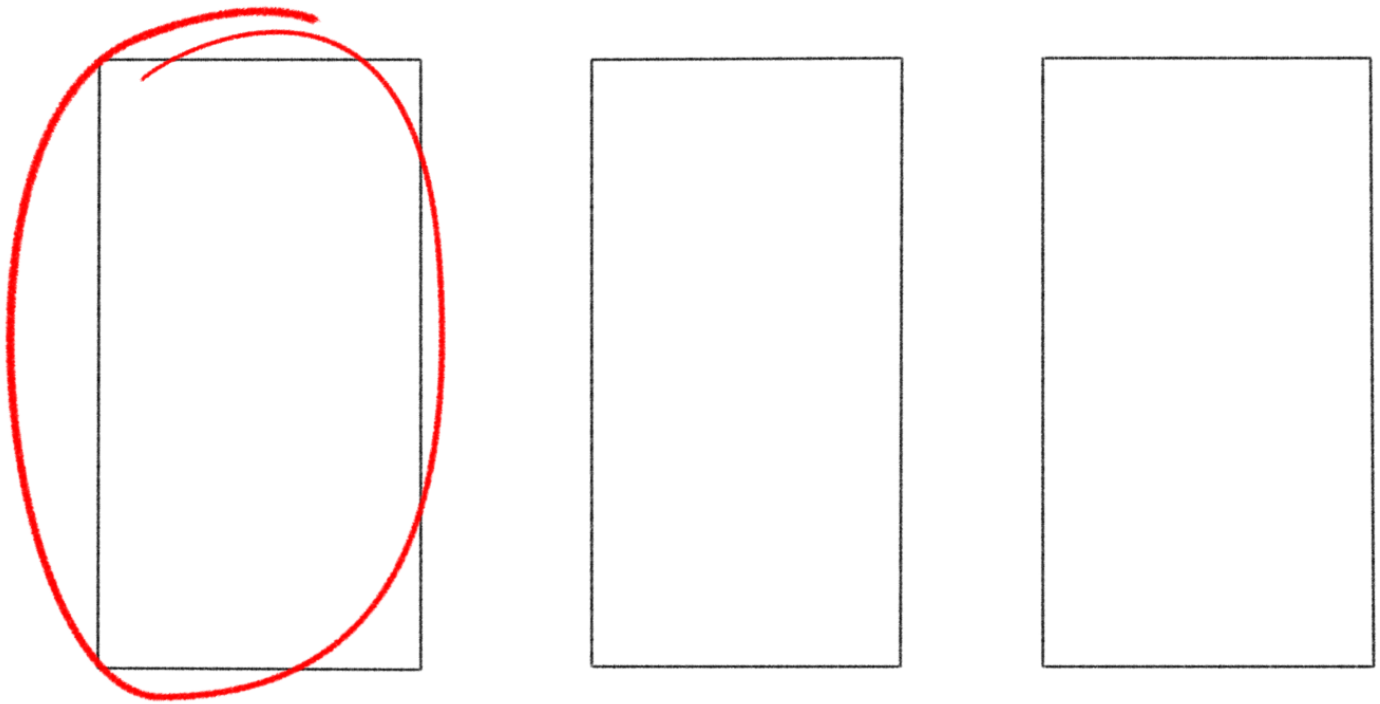
Plan of the talk

Believing Monty Hall

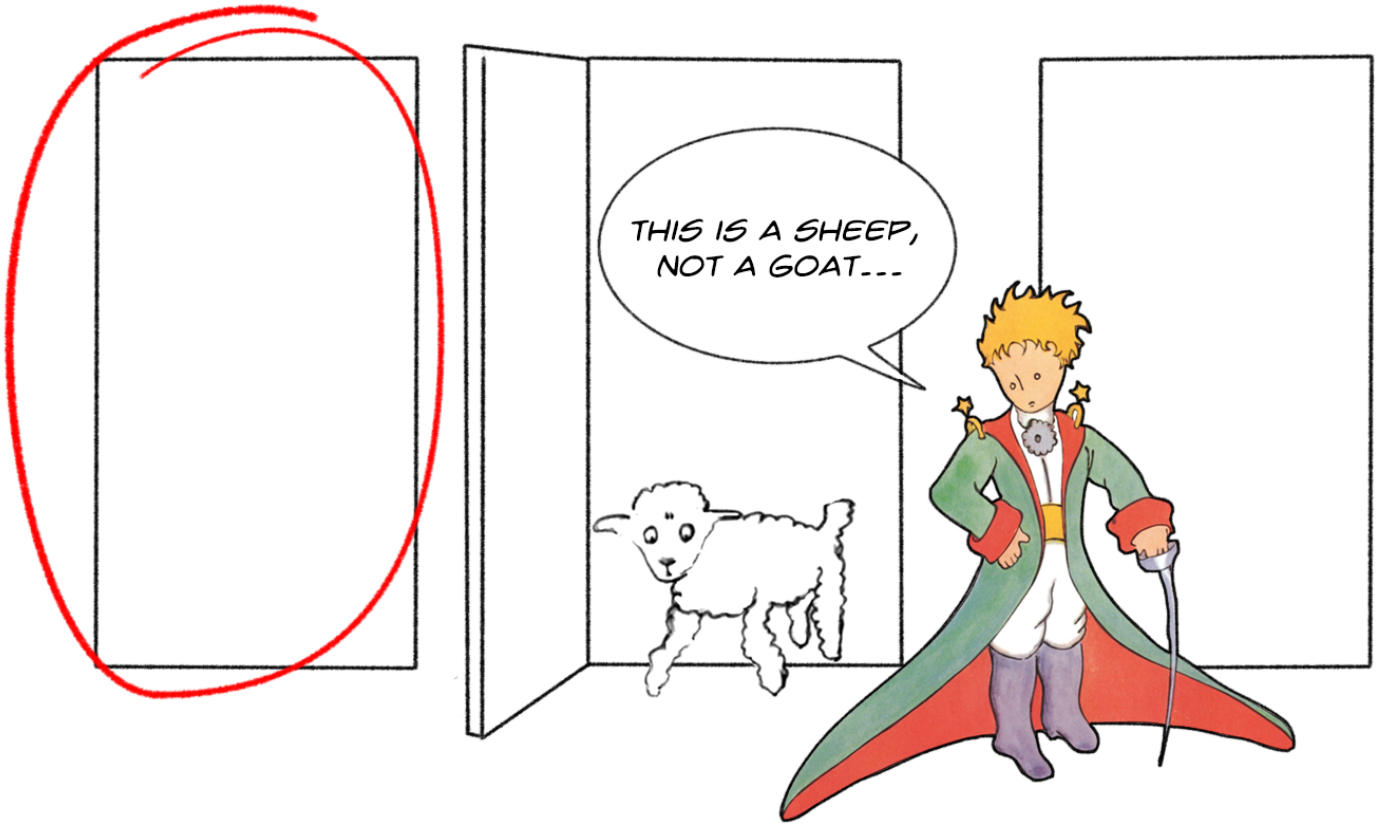
The Monty Hall Problem



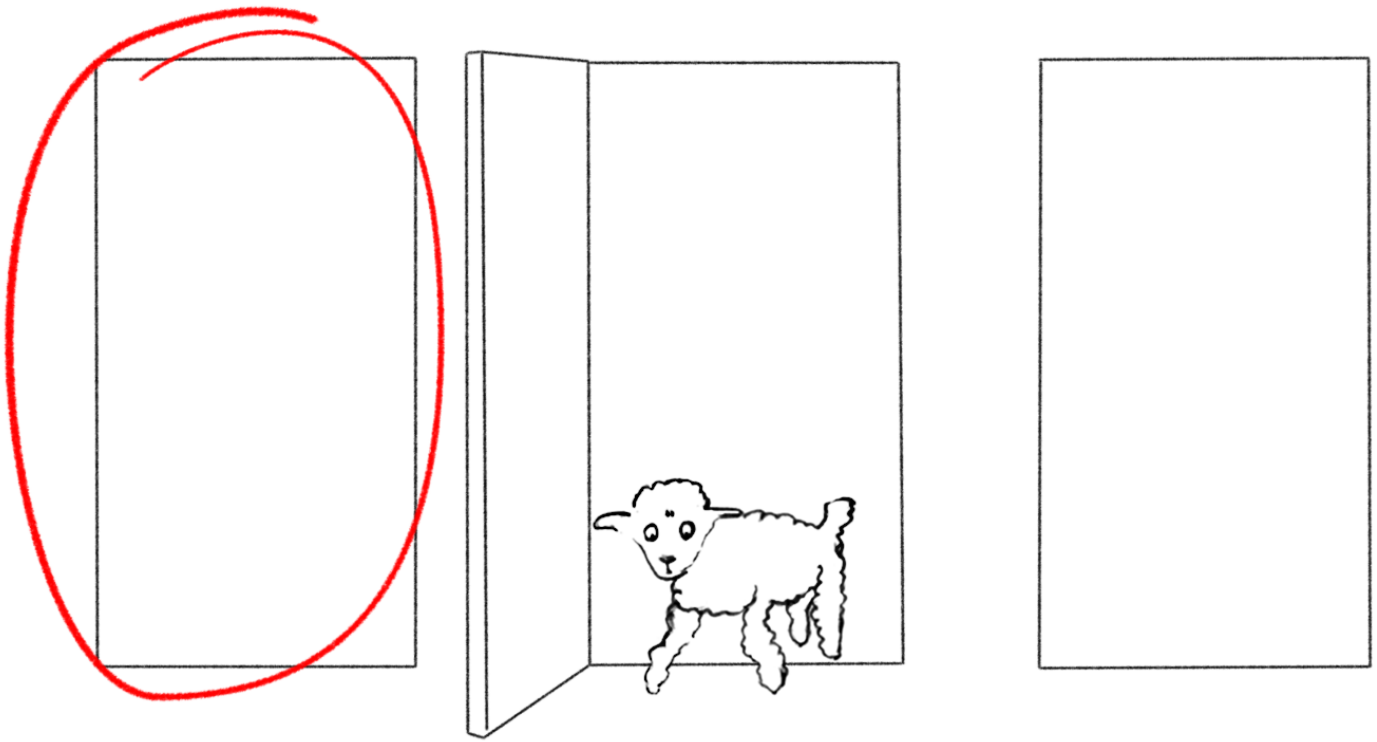
The Monty Hall Problem



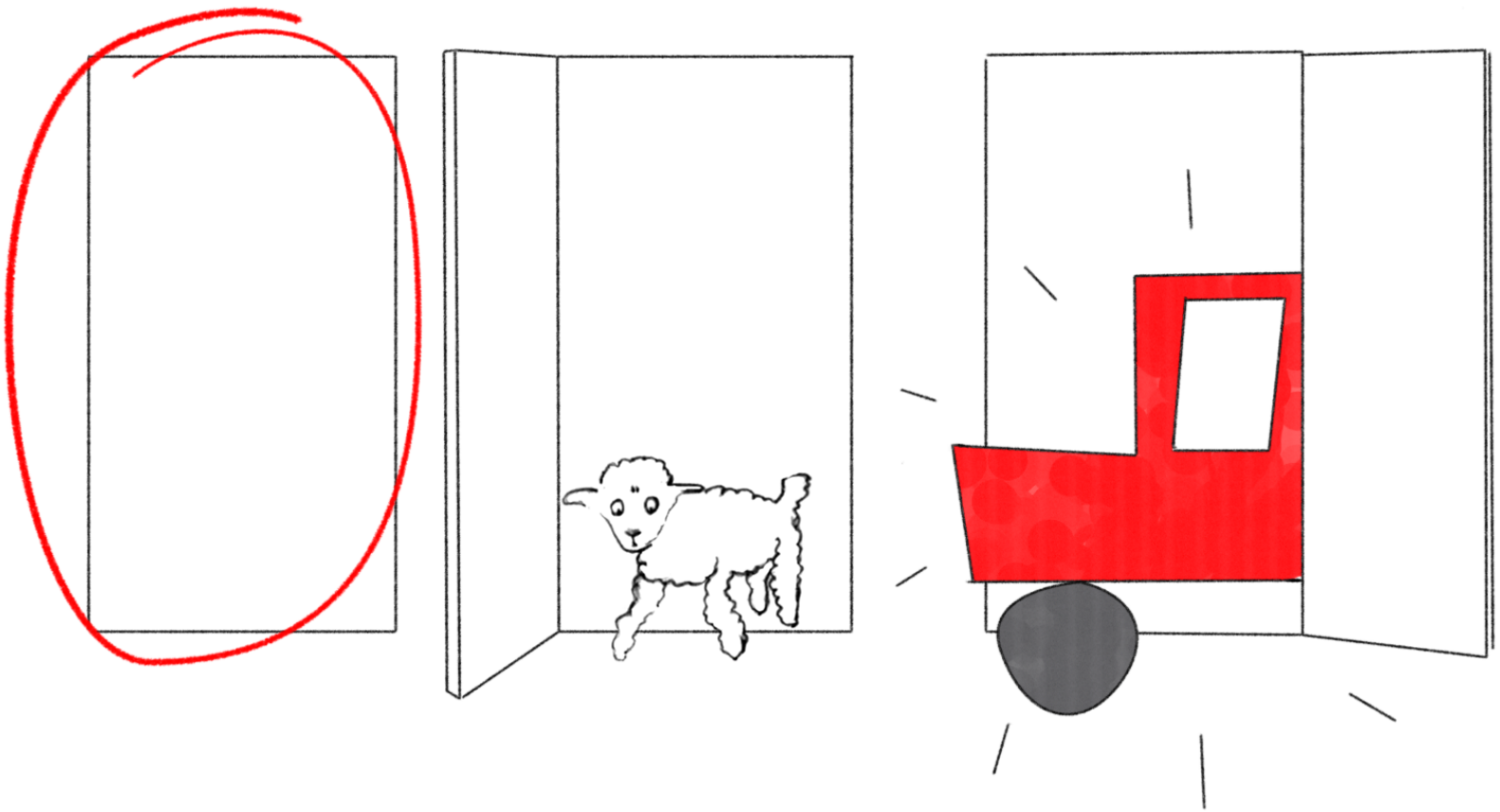
The Monty Hall Problem



The Monty Hall Problem



The Monty Hall Problem



The Monty Hall Problem

Switching is very counter-intuitive

- More than 10000 complaints from readers
- Close to 1000 from people with PhDs

The Monty Hall Problem

Switching is very counter-intuitive

- More than 10000 complaints from readers
- Close to 1000 from people with PhDs

Theorem (Gardner, 1959)

In no other branch of mathematics is it so easy for experts to blunder as in probability theory.

The Monty Hall Problem

People don't agree with Monty Hall

- Minimal and no consequence on real world
- People still refuse to believe the solution

The Monty Hall Problem

People don't agree with Monty Hall

- Minimal and no consequence on real world
- People still refuse to believe the solution

Politics based on probabilities

- Huge consequences and risks
- Higher trust threshold
- No reason to believe it's easier than Monty Hall

Sortition and the Athenians

The Boulê

Citizen's Assembly

- Uses randomly selected citizens (serving one year each)
- Takes decisions on a diveristy of subjects

The Boulê

Citizen's Assembly

- Uses randomly selected citizens (serving one year each)
- Takes decisions on a diveristy of subjects

Voting

- Influence peddling possible
- Votes are not secret

The Heliaia

Justice Court

- Used for most trials
- Jury of random citizens selected in the morning

The Heliaia

Justice Court

- Used for most trials
- Jury of random citizens selected in the morning

Trial conditions

- No interaction with outside world until the end
- Trials last 6 hours at most

Sortition today

Sortition not directly usable in our societies

- Logistical problems

Sortition today

Sortition not directly usable in our societies

- Logistical problems
- Privacy problems

Sortition today

Sortition not directly usable in our societies

- Logistical problems
- Privacy problems
- Trials last more than a day

Sortition today

Sortition not directly usable in our societies

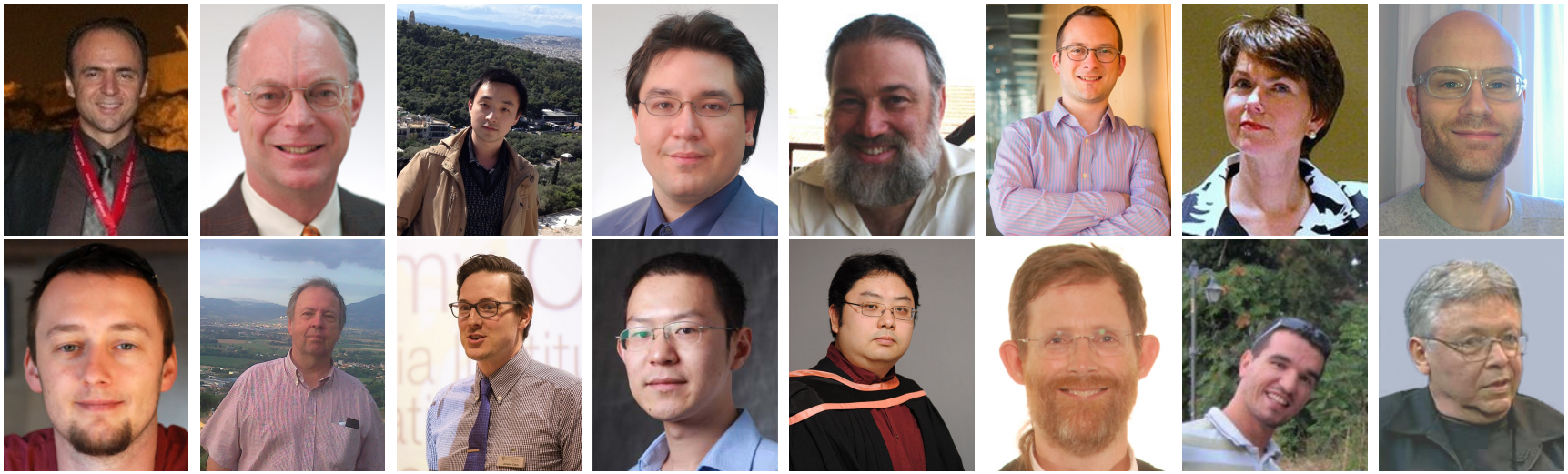
- Logistical problems
- Privacy problems
- Trials last more than a day

Fact

Giving power to a limited set of people is dangerous.

Random Sample Voting

The Random Sample Voting Project Team



Aggelos Kiayias
Deborah Hurley
James Honaker
Neal McBurnett
Peter Schwabe
Emin Gun Sirer
Filip Zagorski
David Parkes

Douglas Wikström
Maciej Kosarzecki
Markus Duermuth
Michael Clarkson
Richard Carback
Pance Ribarski
Alan Sherman
Christof Paar

David Chaum
Hannu Nurmi
Jeremy Clark
Brian Sutin
Mark Ryan
Lirong Xia
Paul Tylkin
Nan Yang

Konstantinos Patsourakos
Pedro A. D. de Rezende
Nicolas K. Blanchard
Tomasz M. Wlisłocki
Christopher Nguyen
Douglas Wikström
Bingsheng Zhang

Client-side protocol

Simplified Protocol

1. Register on the voting lists
2. Get chosen at random in the population
3. Receive a ballot with a unique ID and two vote codes
4. Log in and cast your vote
5. Check that the other code hasn't been used

Constraints

Three constraints to satisfy

Constraints

Three constraints to satisfy

1 : The sampling is demonstrably fair

Constraints

Three constraints to satisfy

1 : The sampling is demonstrably fair

2 : The voting is provably secure

Constraints

Three constraints to satisfy

1 : The sampling is demonstrably fair

2 : The voting is provably secure

3 : The protocol actively prevents corruption

Fair sampling

Public Roster

- Publish list of citizen-number pairs

Fair sampling

Public Roster

- Publish list of citizen-number pairs
- Use Public Random Beacon Bits (NYSE) for the seed

Fair sampling

Public Roster

- Publish list of citizen-number pairs
- Use Public Random Beacon Bits (NYSE) for the seed
- Random Number generator outputs the sample

Fair sampling

Public Roster

- Publish list of citizen-number pairs
- Use Public Random Beacon Bits (NYSE) for the seed
- Random Number generator outputs the sample
- Everyone can check the fairness

Fair anonymous sampling

Encrypted Roster

- Random permutation is initially applied

Fair anonymous sampling

Encrypted Roster

- Random permutation is initially applied
- Encrypted table is published

Fair anonymous sampling

Encrypted Roster

- Random permutation is initially applied
- Encrypted table is published
- Random bits are used to create the sample

Fair anonymous sampling

Encrypted Roster

- Random permutation is initially applied
- Encrypted table is published
- Random bits are used to create the sample
- Key is released after voting

Fair anonymous sampling

Encrypted Roster

- Random permutation is initially applied
- Encrypted table is published
- Random bits are used to create the sample
- Key is released after voting
- Members are kept anonymous during the vote

Secure voting

Theorem (J. Stalin, 1923, origin disputed)

It's not the people who vote that count, but those who count the vote.

Secure voting

End-to-End verifiability

- Voters can't prove what they voted for
- Voters can be sure that their vote was correctly counted
- No ballots can be added, modified or removed

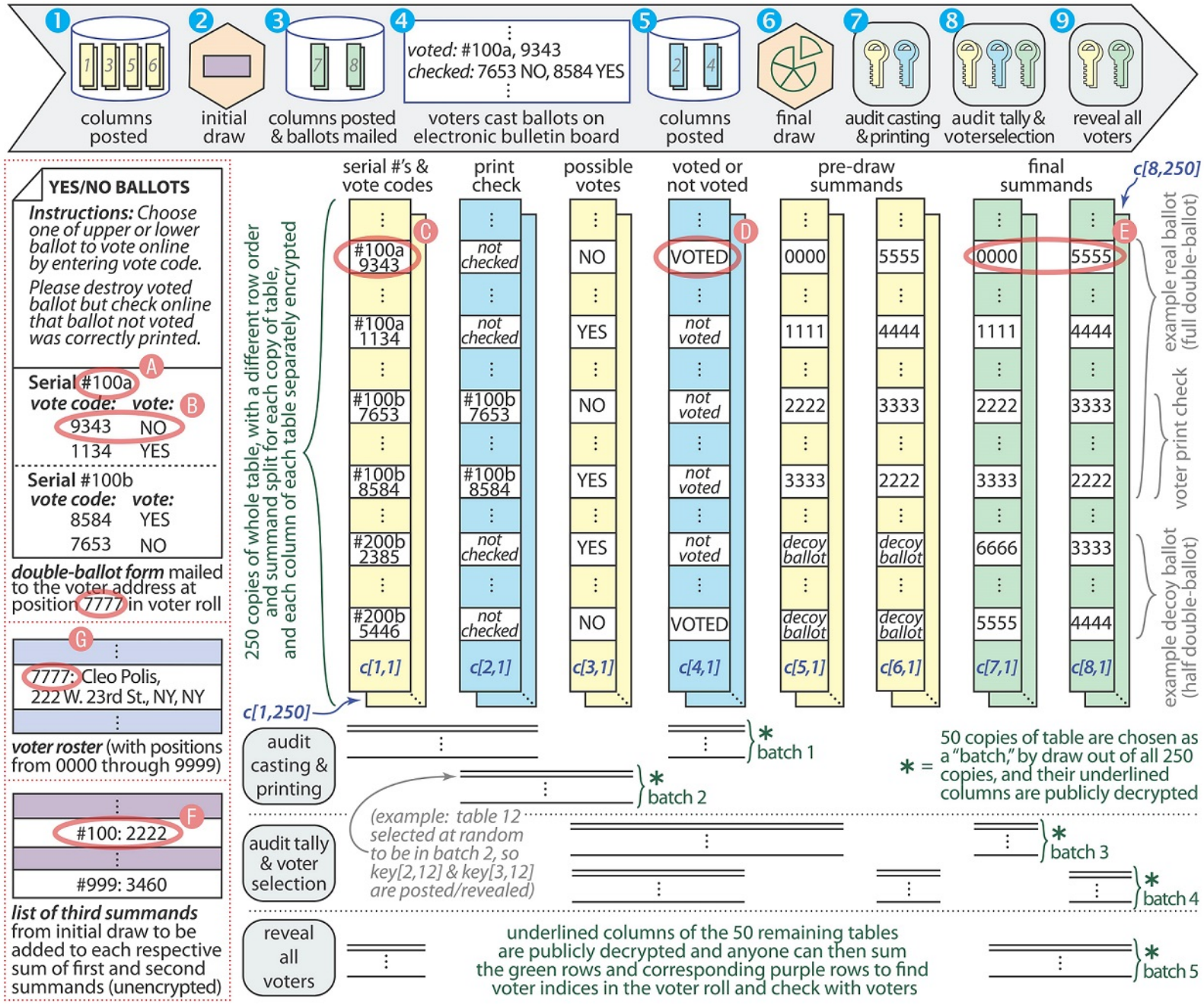
Secure voting

End-to-End verifiability

- Voters can't prove what they voted for
- Voters can be sure that their vote was correctly counted
- No ballots can be added, modified or removed

Multiple step process

- Create permuted versions of the enriched roster
- Encrypt them with different keys
- Selectively reveal certain columns of certain tables
- The (table-column) couple depends on public coins


1 columns posted
2 initial draw
3 columns posted & ballots mailed
4 voted: #100a, 9343
checked: 7653 NO, 8584 YES
voters cast ballots on electronic bulletin board
5 columns posted
6 final draw
7 audit casting & printing
8 audit tally & voterselection
9 reveal all voters
YES/NO BALLOTS
Instructions: Choose one of upper or lower ballot to vote online by entering vote code.
Please destroy voted ballot but check online that ballot not voted was correctly printed.
A
Serial #100a
vote code: vote:
B
9343 NO
1134 YES
Serial #100b
vote code: vote:
8584 YES
7653 NO
double-ballot form mailed to the voter address at position 7777 in voter roll
G
7777: Cleo Polis, 222 W. 23rd St., NY, NY
voter roster (with positions from 0000 through 9999)
F
#100: 2222
#999: 3460
list of third summands from initial draw to be added to each respective sum of first and second summands (unencrypted)
250 copies of whole table, with a different row order and summand split for each copy of table, and each column of each table separately encrypted
serial #'s & vote codes
print check
possible votes
voted or not voted
pre-draw summands
final summands
c[8,250]
C
D
E
#100a 9343
#100a 1134
#100b 7653
#100b 8584
#200b 2385
#200b 5446
not checked
NO
YES
VOTED
not voted
0000
1111
2222
3333
5555
4444
6666
decoy ballot
c[1,1]
c[2,1]
c[3,1]
c[4,1]
c[5,1]
c[6,1]
c[7,1]
c[8,1]
c[1,250]
example real ballot (full double-ballot)
voter print check
example decoy ballot (half double-ballot)
audit casting & printing
batch 1
batch 2
* = 50 copies of table are chosen as a "batch," by draw out of all 250 copies, and their underlined columns are publicly decrypted
audit tally & voter selection
(example: table 12 selected at random to be in batch 2, so key[2,12] & key[3,12] are posted/revealed)
batch 3
batch 4
reveal all voters
underlined columns of the 50 remaining tables are publicly decrypted and anyone can then sum the green rows and corresponding purple rows to find voter indices in the voter roll and check with voters
batch 5

The problem of corruption

Traditional corruption & coercion

- Give money or advantages to some voters
- Check who votes and threaten them

The problem of corruption

Traditional corruption & coercion

- Give money or advantages to some voters
- Check who votes and threaten them

With RSV

- Anonymous sample, so hard to target people to bribe
- Secret secure ballot so threatening is hard

The problem of corruption

Traditional corruption & coercion

- Give money or advantages to some voters
- Check who votes and threaten them

With RSV

- Anonymous sample, so hard to target people to bribe
- Secret secure ballot so threatening is hard

- Changes the market from buyer-focused to seller-focused

Decoy ballots

Additional decoy ballots

- Looks in all ways identical to real ballot
- Provably a decoy (impossible to prove authenticity of ballots)
- Is not counted in the final tally

Decoy ballots

Additional decoy ballots

- Looks in all ways identical to real ballot
- Provably a decoy (impossible to prove authenticity of ballots)
- Is not counted in the final tally

Effects

- Market saturated in decoys
- People with decoys will try to trick buyers
- Huge risk, smaller reward : low incentive to buy votes

Distributing the decoys

Random distributions

- Uniform is fair, but no real advantage if people are corrupt
- Biased distribution can protect against massive buyer budget
- Even a small proportion of decoys are enough

Distributing the decoys

Random distributions

- Uniform is fair, but no real advantage if people are corrupt
- Biased distribution can protect against massive buyer budget
- Even a small proportion of decoys are enough

Civic duty defense

- Anyone can request a decoy
- Extremely close to optimal defense
- Good for large populations

Advantages of RSV

Technical advantages

- Mathematically secure
- Easy to use
- Inexpensive

Advantages of RSV

Technical advantages

- Mathematically secure
- Easy to use
- Inexpensive

Probable social advantages

- Increased participation
- More informed voters
- Can form the basis for real modern direct democracy

Building Trust

RSV In Practice

Expert trials

- Tested at Crypto 2015 and Real World Crypto 2016
- Data and audits publicly available
- No vulnerabilities found
- Publicity within the field

Problem

We still needed a real public trial

Global Forum on Modern Direct Democracy

GFMDD '16 in San Sebastian

- Around 200 participants from more than 30 countries for four days
- Journalists, political scientists, politicians, local activists

Global Forum on Modern Direct Democracy

GFMDD '16 in San Sebastian

- Around 200 participants from more than 30 countries for four days
- Journalists, political scientists, politicians, local activists

RSV at the forum

- Two parallel votes, around 120 ballots total :
  - Should voting be mandatory ?
  - Should negative campaigning be authorized ?

Murphy's Law

Technical problems

- Printing ballots
- HTML on certain devices

Murphy's Law

Technical problems

- Printing ballots
- HTML on certain devices

Design issues

- Font problems
- Voting timeline

Results from GFMDD

Participation

- Around 25-30% average
- Highly dependent on the question

Results from GFMDD

Participation

- Around 25-30% average
- Highly dependent on the question

Feedback from voters

- Found easy to use and trustworthy (from a security standpoint)
- Not as legitimate as general elections, but would increase engagement
- Mixed opinions about corruption prevention

Creating Familiarity

Trust vicious cycle

- Without successful large scale trials, system isn't seen as trustworthy or legitimate
- Without legitimacy, people won't use the system
- If people don't use it, no large scale trials are possible

Creating Familiarity

Trust vicious cycle

- Without successful large scale trials, system isn't seen as trustworthy or legitimate
- Without legitimacy, people won't use the system
- If people don't use it, no large scale trials are possible

Improving intuition

- Best method is experimentally (as with betting)
- RSV Simulator

RSV Simulator

Features

- Past elections to confirm correctness
- Simple and advanced modes
- Security and authenticity by having all code run on the machine
- Viewable temporarily at www.koliaza.com/rsvp

The Public Opinion Platform

What is POP

A Platform and a Party

- Integrate deliberation and voting
- Single promise from representants : follow the will of the people
- International in scope

What is POP

A Platform and a Party

- Integrate deliberation and voting
- Single promise from representants : follow the will of the people
- International in scope

Real-time democracy

- Give people back permanent control
- Doesn't need support from governments
- Can progressively transform the political scene

POP Special Exploratory Committee

Bruno
Kaufmann
Reporter
SwissInfo

Diana
Wallis
Member and ex-VP
EU Parliament

Géza
Tessényi
Legal scholar
Council of Europe

Gudmundur
Alfredsson
Professor
CUPSL

Nicolas K.
Blanchard
Doctoral student
IRIF/RSVP

POP and RSV

Establishing legitimacy

- Secure voting system
- Avoid self-selection and represent the whole people
- Also improves visibility

POP and RSV

Establishing legitimacy

- Secure voting system
- Avoid self-selection and represent the whole people
- Also improves visibility

Making it accessible

- Increasing local and global participation
- Bridging the digital gap through third party voting

The Future

Improving RSV

Design

- Central voting site to simplify parallel votes
- Simpler crypto-system
- User-friendly scratch-off ballots

Improving RSV

Design

- Central voting site to simplify parallel votes
- Simpler crypto-system
- User-friendly scratch-off ballots

Public appeal

- Larger scale trials
- Improved simulator
- Free-to-use voting website for people to try

Fighting for POP

Improving POP

- System still being implemented
- Reflexions on best access methods and evolution
- Platform/RSV balance to be found

Fighting for POP

Improving POP

- System still being implemented
- Reflexions on best access methods and evolution
- Platform/RSV balance to be found

Making it POPular

- Reluctance from political class
- Thanks to RSV, grassroots is possible
- About to go public

Collaborations

RSV

- Council of Europe for major vote at WFD
- Efforts to study impact on abstention with Herrade Igersheim

Collaborations

RSV

- Council of Europe for major vote at WFD
- Efforts to study impact on abstention with Herrade Igersheim

POP

- Appeal to politicians in multiple countries
- Work with Council of Europe
- Technology exchange with vTaiwan and Pol.is