Decentralized Governance

David Chaum (xx network see chaum.com)

Outline

"More money more votes" is easy online & decentralized:

- Public vote (digital sigs)
- Private vote (+mixing)

(but not "secret ballot")

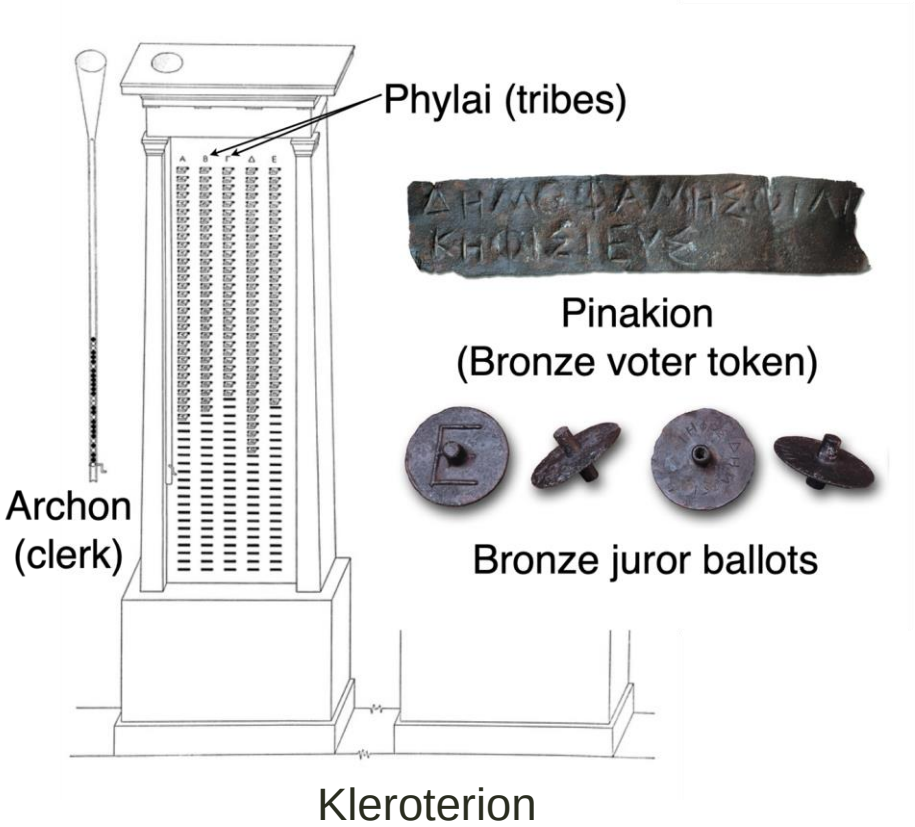
"One person one vote"* (i.e., improper influence protection) is ***hard*** online and harder decentralized, but we have made *breakthroughs:*

(1) Decoy ballots: RSvoting.org

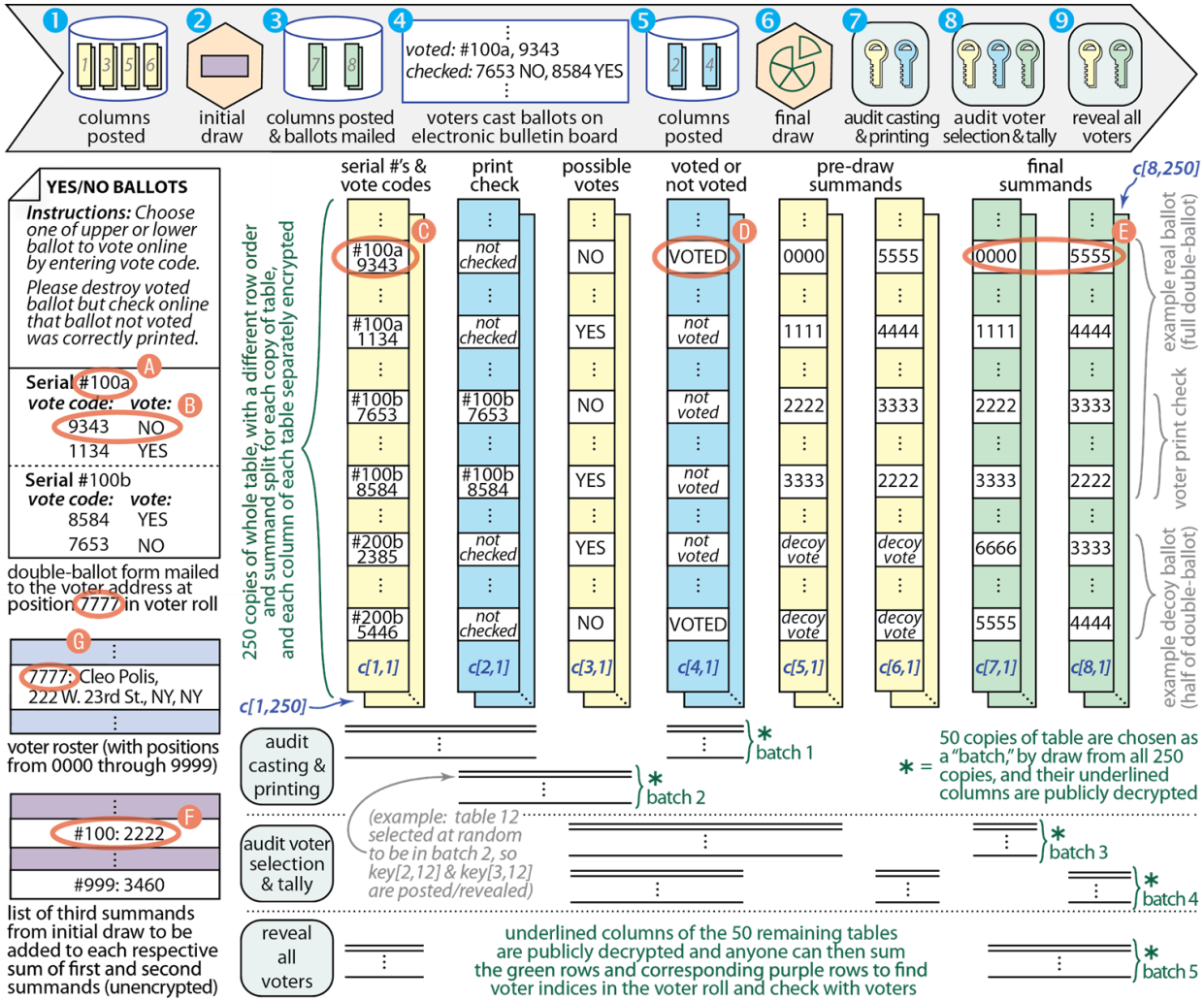
(2) Nullification protocol: Votexx.org

* Whatever the electoral rules

Athenian Juries



RSVoting.org (“decoy ballots”)


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 voter selection & tally
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
decoy vote
6666
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 of double-ballot)
audit casting & printing
batch 1
batch 2
audit voter selection & tally
(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
* = 50 copies of table are chosen as a "batch," by draw from all 250 copies, and their underlined columns are publicly decrypted

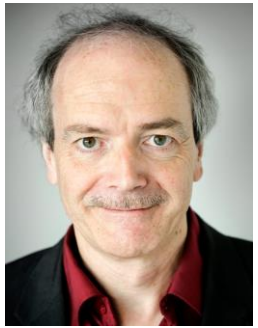
VOTEX.org ("nullification")

David Chaum
xx network

Jeremy Clark
U Concordia

Chao Liu
UMBC

Mahdi Nejadgholi
U Concordia

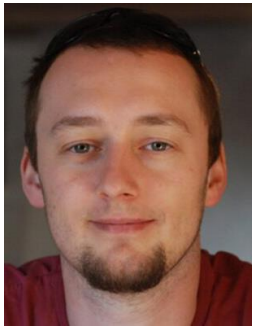


Bart Preneel
KU Leuven

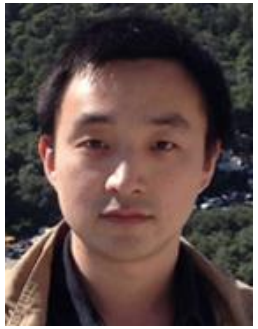
Rick T. Carback
xx network

Alan T. Sherman
UMBC

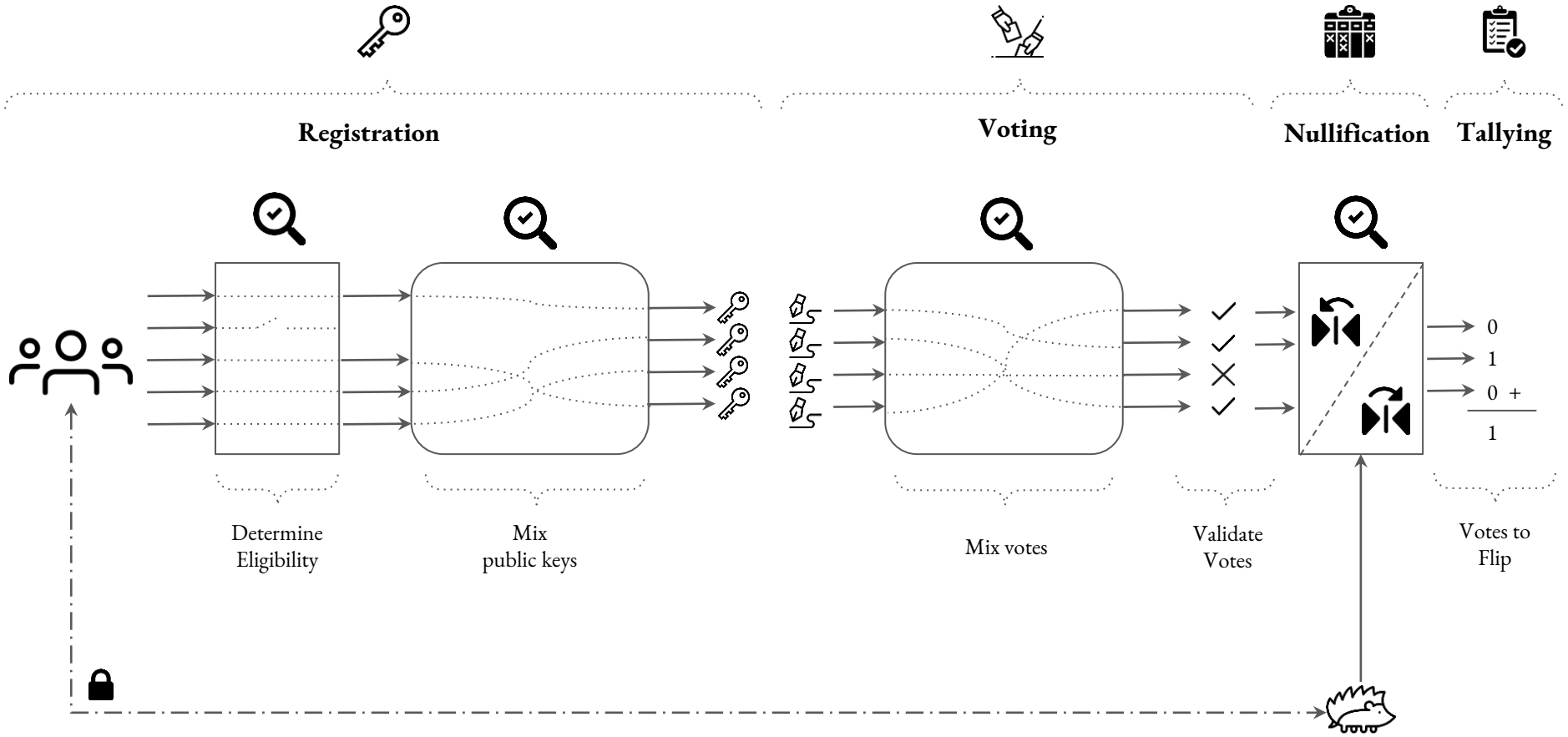
Mario Yaksetig
xx network



Filip Zagorski
Wrocław UST



Bingsheng Zhang
Zhejiang University


Registration
Voting
Nullification
Tallying
Determine Eligibility
Mix public keys
Mix votes
Validate Votes
0
1
0 +
1
Votes to Flip

Overall elections

please see: Rsvoting.org… *jury voting best according*

(a) high effective voter turnout
(b) better informed voters rationally motivated to delve into issues
(c) increased effectiveness of results in shaping governance
(d) improved resistance to manipulation through advertising/campaigning
(e) increased indisputability and trustworthiness of results
(f) anonymity of voters with unsaleable votes
(g) reduced opportunity for selective denial of voter access
(h) voter fraud only through improper voter rolls
(i) equivalent but safer decisiveness
(j) reduced direct and overall cost

Thank You