

Securing Digital Democracy



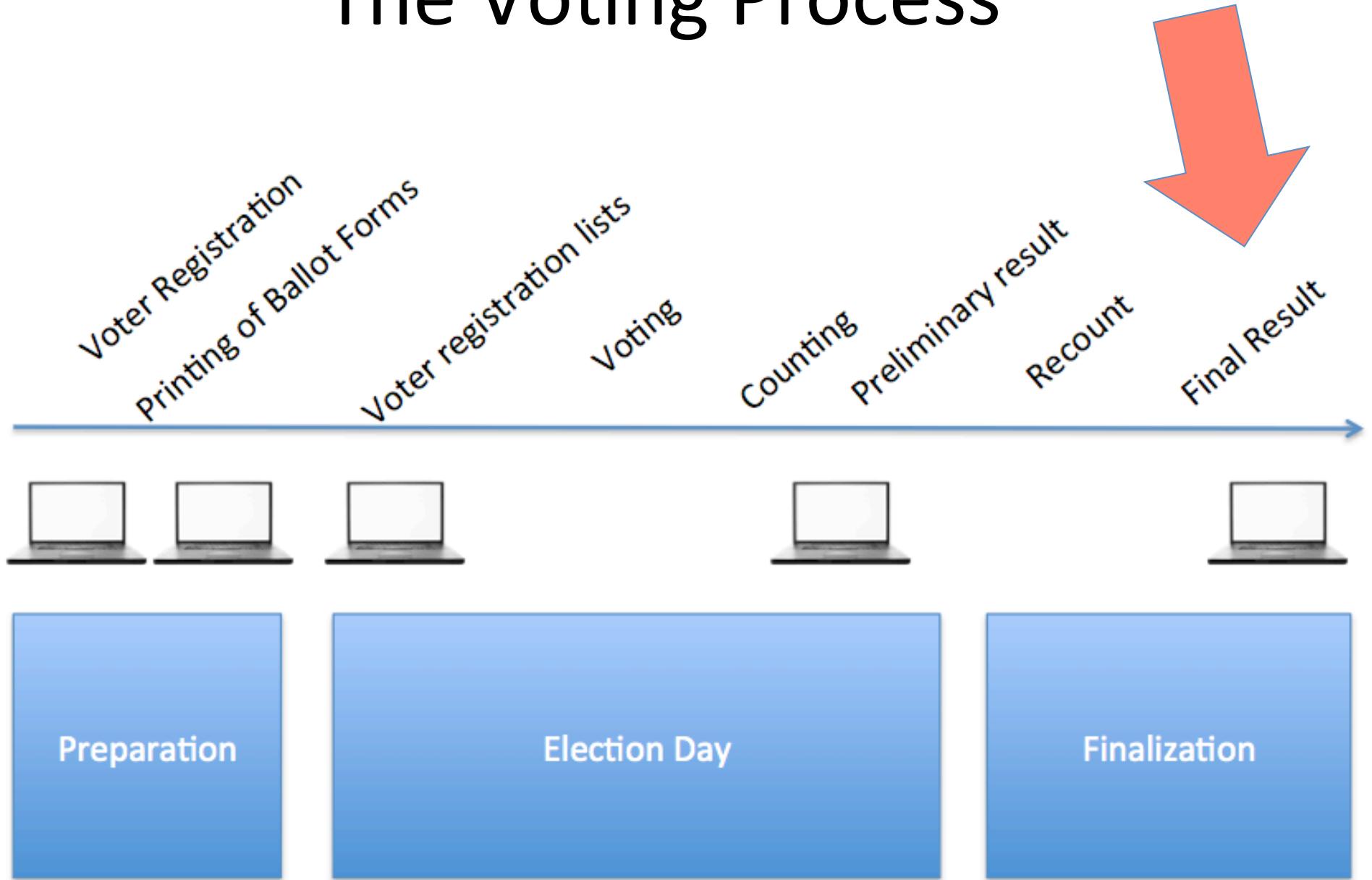
Carsten Schürmann, DemTech, IT University of Copenhagen

All but 11 countries held
national elections since 2000
[Kofi Annan Foundation Report 2012]

Electoral Management Bodies
want to use of technology!



The Voting Process



Electoral System

Social Choice Theory

D'Hondt for (13 Seats)

Party	A	B	C	D	E	F	G	H	I
Total	2220	530	665	750	621	1120	370	335	350

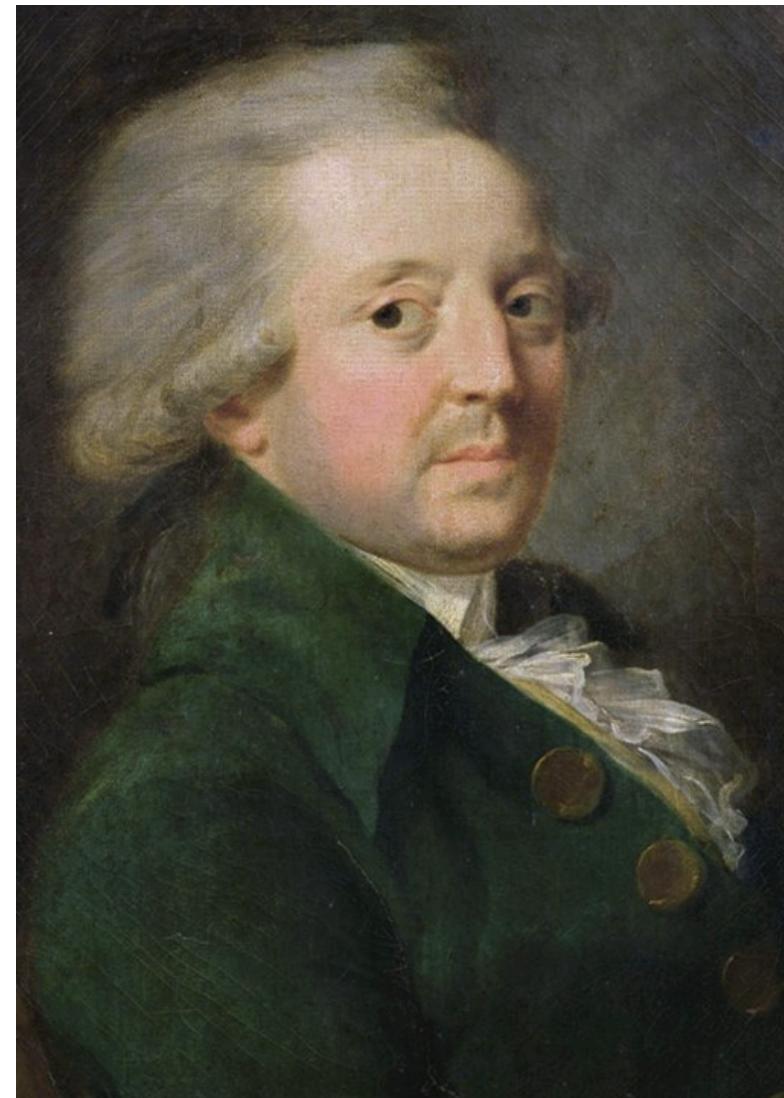
1	2220	1195	750	621	1120	707		350
2	1110	598	375	311	560	354		175
3	740	398	250	207	373	236		117
4	555	299	188	155	280	177		88
5	444	239	150	124	224	114		70
6	370	199	125	104	187	118		58

Party	A	B	C	D	E	F	G	H	I
Seats	5	3		1	1	2	1	0	

Marquis de Condorcet 1743-1794

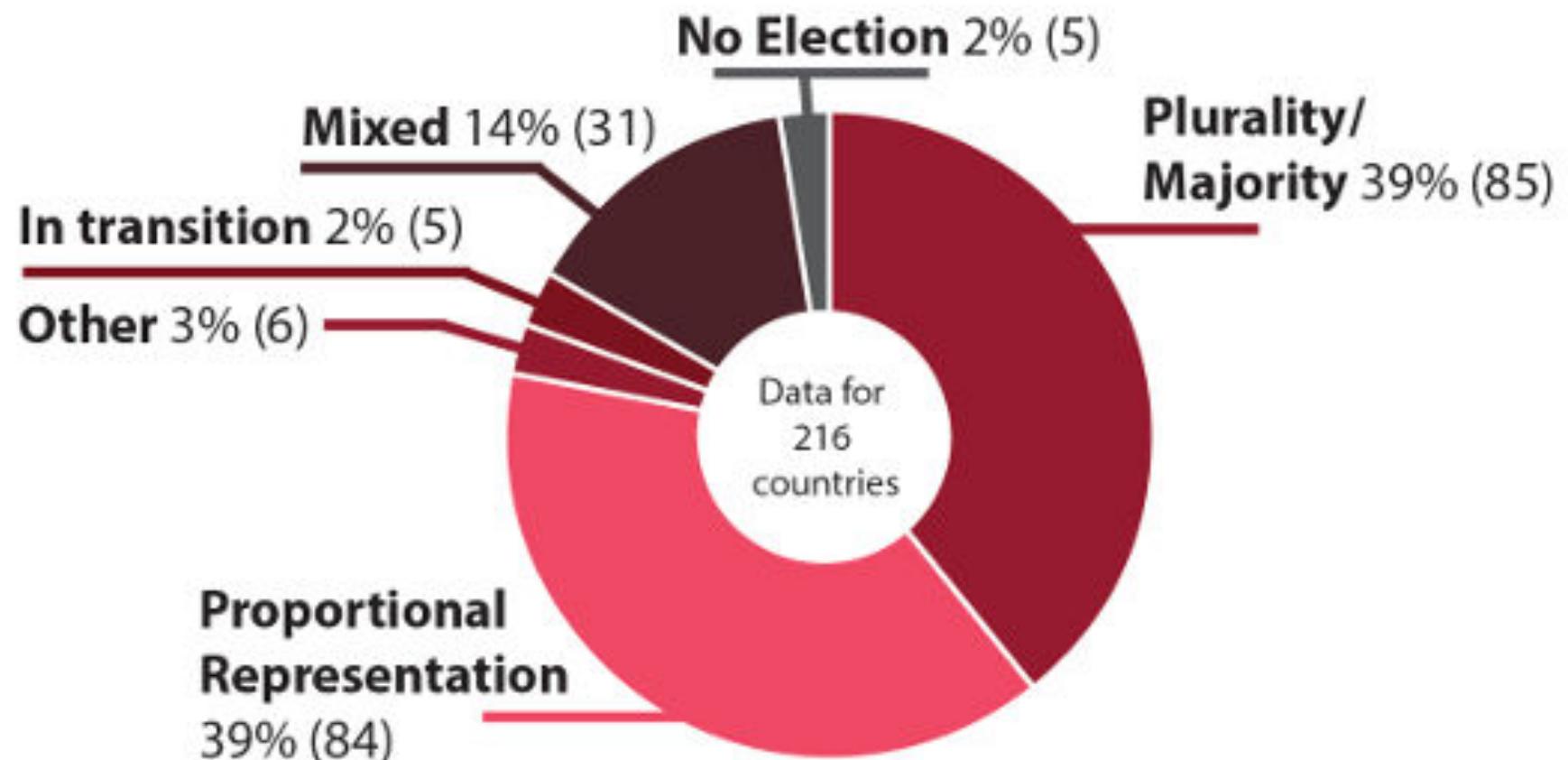
How to do good decisions?

- Algorithms
 - First Past The Post
 - Single Transferable Vote
- Properties
 - Majority
 - Monotonicity
 - Condorcet Winner
- Arrow's impossibility result



	Majority (MC)	Mutual MC	Condorcet	Cond. loser	Smith/ ISDA	IIA	IIA	Cloneproof	Monotone	CC	PC	Reversal symmetry	Polytime/ Resolvable	Summary
Approval	Rated [nb 1]	No	No [nb 2] [nb 3]	No	No [nb 2]	Yes	Yes [nb 4]	Yes [nb 5]	Yes	Yes	Yes	Yes	O(N)	Yes O(N)
Borda count	No	No	No [nb 2]	Yes	No	No	No	No: teams	Yes	Yes	Yes	Yes	O(N)	Yes O(N)
Copeland	Yes	Yes	Yes	Yes	Yes	No	No [nb 2]	teams, crowds	Yes	No [nb 2]	No [nb 2]	Yes	O(N ²)	No O(N ²)
IRV (AV)	Yes	Yes	No [nb 2]	Yes	No [nb 2]	No	No	Yes	No	No	No	No	O(N ²)	Yes O(N! [nb 7])
Kemeny-Young	Yes	Yes	Yes	Yes	Yes	Yes	No [nb 2]	No: spoilers	Yes	No [nb 2]	No [nb 2]	Yes	O(N!)	Yes O(N ² [nb 9])
Majority Judgment [nb 10]	Rated [nb 11]	No [nb 12]	No [nb 2] [nb 3]	No	No [nb 2]	Yes	Yes [nb 4]	Yes	Yes	No [nb 13]	No [nb 14]	Depends [nb 15]	O(N)	Yes O(N [nb 16])
Minimax	Yes	No	Yes [nb 19]	No	No	No	No [nb 2]	No: spoilers	Yes	No [nb 2]	No [nb 2]	No	O(N ²)	Yes O(N ²)
Plurality	Yes	No	No [nb 2]	No	No [nb 2]	No	No	No: spoilers	Yes	Yes	Yes	No	O(N)	Yes O(N)
Range voting	No	No	No [nb 2] [nb 3]	No	No [nb 2]	Yes	Yes [nb 4]	Yes	Yes	Yes	Yes	Yes	O(N)	Yes O(N)
Ranked pairs	Yes	Yes	Yes	Yes	Yes	Yes	No [nb 2]	Yes	Yes	No [nb 2]	No [nb 14]	Yes	O(N ⁴)	Yes O(N ²)
Runoff voting	Yes	No	No [nb 2]	No	No [nb 2]	No	No	No: spoilers	No	No	No	No	O(N) [nb 21]	Yes O(N [nb 22])
Schulze	Yes	Yes	Yes	Yes	Yes	No	No [nb 2]	Yes	Yes	No [nb 2]	No [nb 14]	Yes	O(N ³)	Yes O(N ²)

Electoral Systems Families



Source: International IDEA, 2015

Electoral System Innovation

- Social welfare
- Governance
- Fairness
- Trust

*Negative Vote Weight
[Supreme Court Germany]*

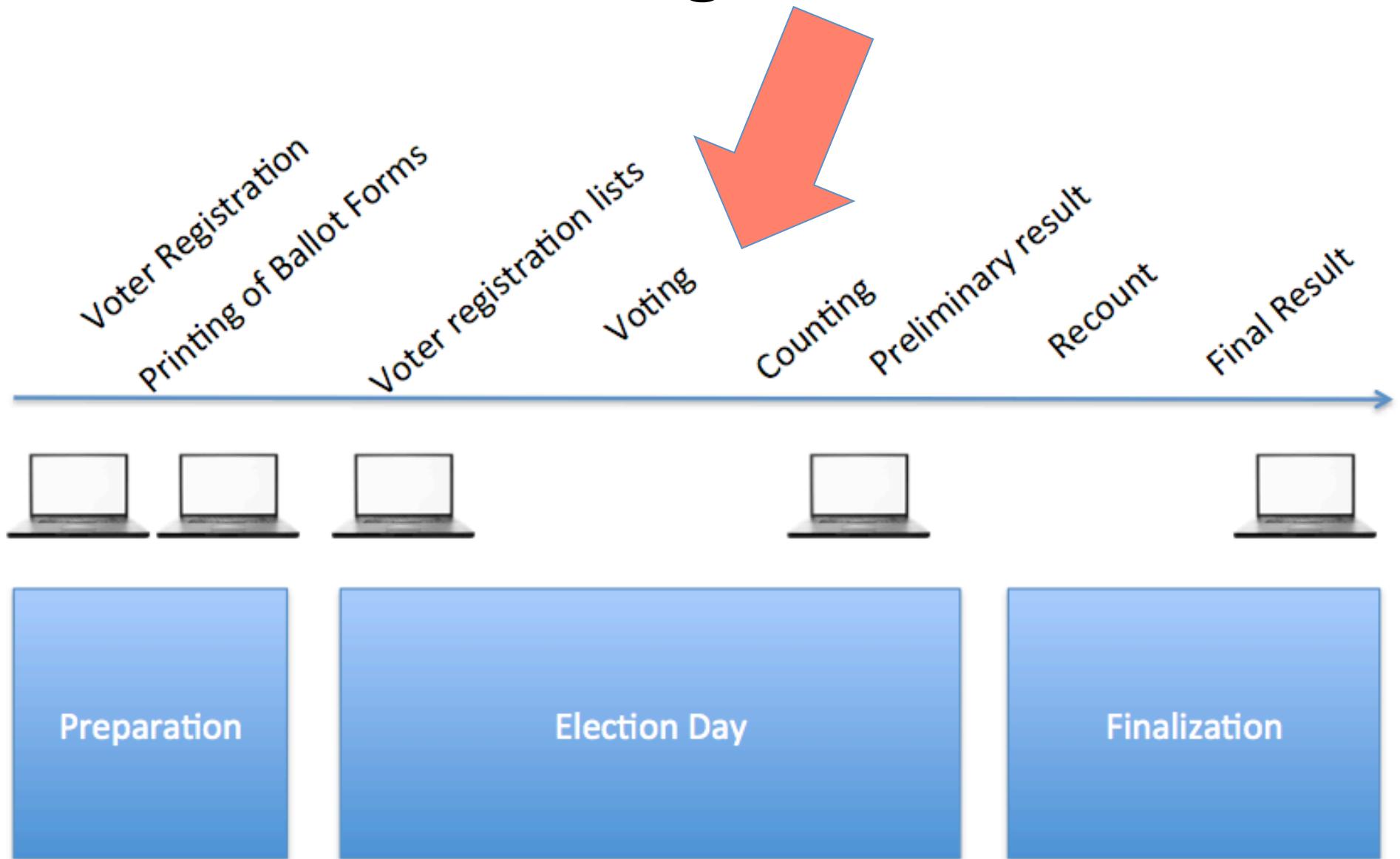
“Double Pukkelsheim”

This formula determines the result of the “Kantonrats” election next weekend. It increases the likelihood for small parties to gain seats.



TagesAnzeiger Zurich, 2007

The Voting Process



Voting Technology

Electronic Voting in Denmark

L-132

[12/13]

- Intended to authorize the use of electronic voting machines
- No internet elections

No majority in Folketinget

FOLKETINGSTIDENDE A

FOLKETINGET



Lovforslag nr. L 132

Folketinget 2012-13

Fremsat den 31. januar 2013 af økonomi- og indenrigsministeren (Margrethe Vestager)

Forslag

til

Lov om ændring af lov om valg til Folketinget, lov om valg af danske medlemmer til Europa-Parlamentet og lov om kommunale og regionale valg

(Digital stemmeafgivning og stemmeoptælling m.v.)

§ 1

I lov om valg til Folketinget, jf. lovbekendtgørelse nr. 107 af 8. februar 2011, som ændret ved lov nr. 251 af 21. marts 2012, lov nr. 589 af 18. juni 2012 og § 3 i lov nr. 1252 af 18. december 2012, foretages følgende ændringer:

1. Efter kapitel 9 indsættes:

»Kapitel 9 a

Digital stemmeafgivning og stemmeoptælling m.v.

§ 74 b. Økonomi- og indenrigsministeren kan forud for et folketingsvalg efter ansøgning give en kommunalbestyrelse tilladelse til, at stemmeafgivningen i kommunen, stemmeoptællingen eller begge dele sker digitalt. Tilladelsen kan begrænses til et eller flere afstemningssteder eller brevstemmeafgivningssteder. Økonomi- og indenrigsministeren kan fastsætte vilkår for tilladelsen. Økonomi- og indenrigsministeren kan herunder fastsætte vilkår om, hvilket eller hvilke af de i madfør af stk. 2 navede customer kommunen kan

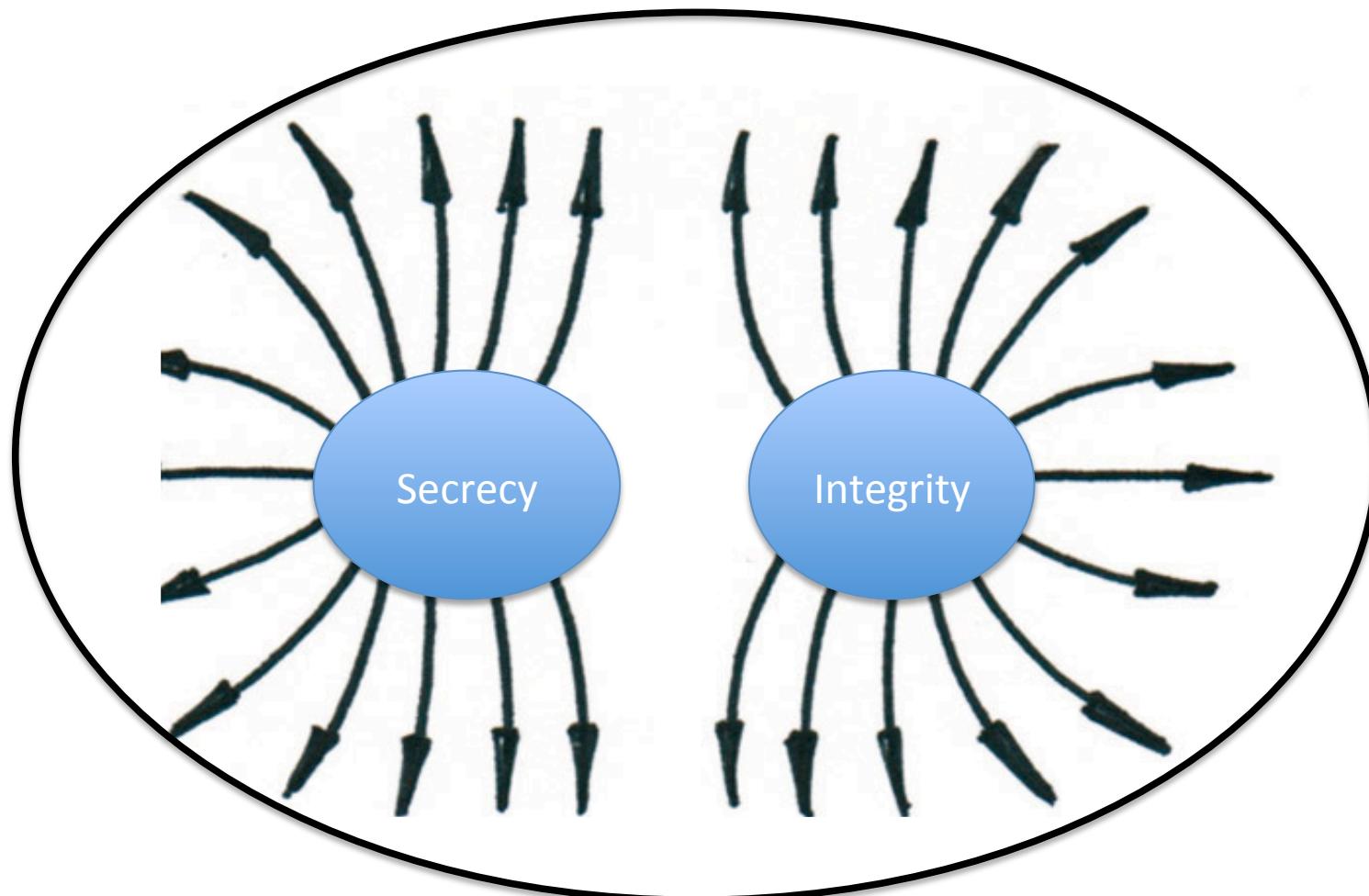
st. 1, afholdelse af udbud efter st. 2 og fastsættelse af regler efter st. 3 foretage de nødvendige fravigelser af

- 1) § 14, stk. 1,
- 2) § 23, stk. 2,
- 3) § 33 a, stk. 2, 2.-5. pkt., § 39, stk. 2, § 40, stk. 2, §§ 43 og 44,
- 4) § 45, stk. 2, 4. pkt., og stk. 3, § 46, stk. 2, § 47, 7. pkt., § 48, stk. 1, 2. pkt., stk. 2 og 3, § 49, stk. 4, og § 52,
- 5) § 60, stk. 1 og 2, § 61, stk. 1, 2. pkt., stk. 2 og 3, stk. 4, 1. og 3. pkt., stk. 6 og 7, § 64, stk. 1, 1. pkt., stk. 2 og 4-6, § 65, stk. 1 og stk. 2, nr. 3-5, og § 66, samt
- 6) § 68, § 69, stk. 1-3, §§ 71 og 72, § 73, stk. 1-4 og 6, og § 74.«

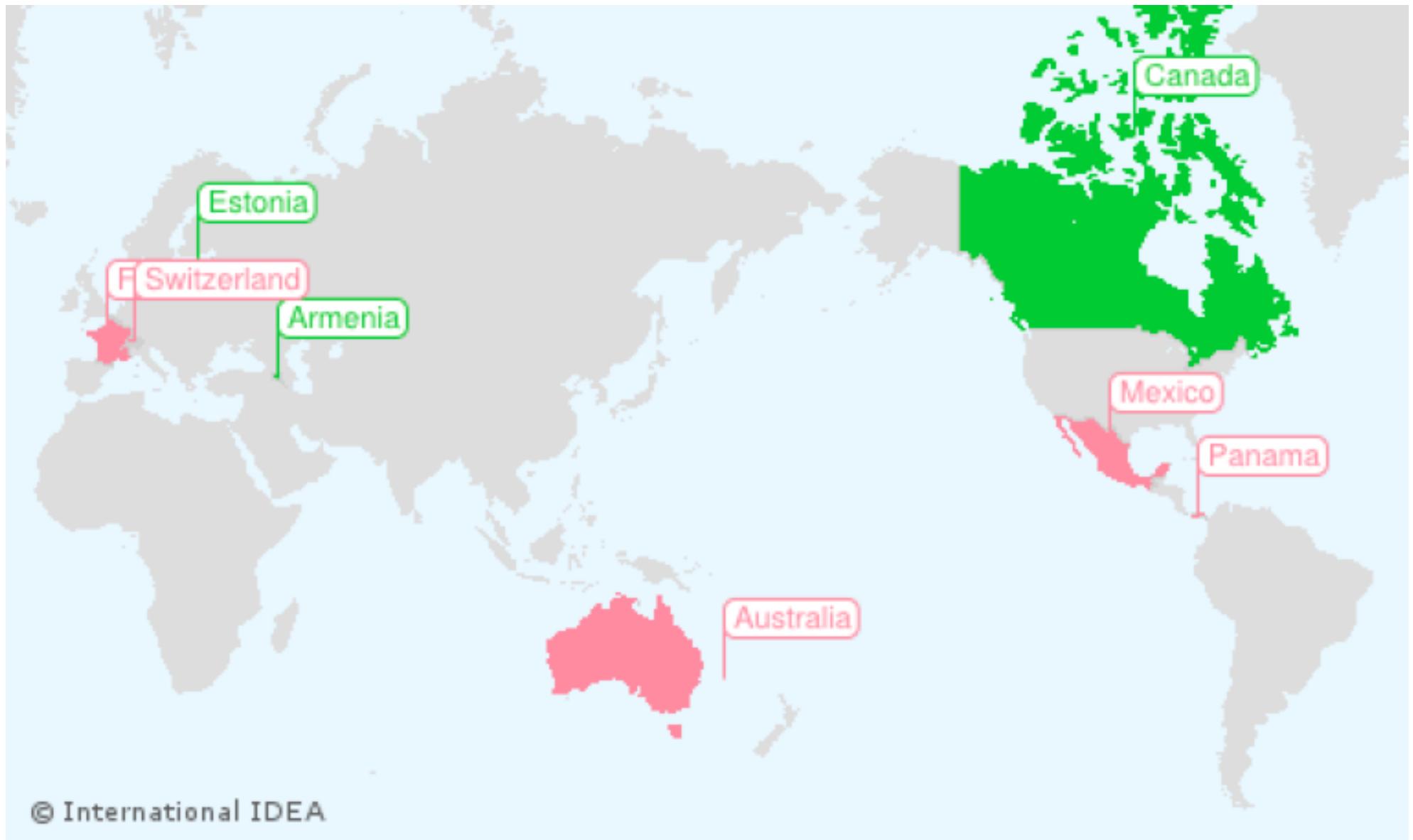
2. Efter § 101 indsættes:

»§ 101 a. Økonomi- og indenrigsministeren kan forud for en folkeafstemning efter ansøgning give en kommunalbestyrelse tilladelse til, at stemmeafgivningen i kommunen, stemmeoptællingen eller begge dele sker digitalt. Tilladelsen kan

Technical Challenge



National Binding Internet Elections



More and More Countries Consider It!

- Geographic challenges
- Inclusion of eligible voters living abroad
- Hope for increased voter turnout
- Hope to encourage young voters to vote
- Cost saving

Lithuanian parliament to discuss legalizing online voting in elections

Submitted by AGORA moderator on 10 February 2015



VILNIUS, Feb. 9 (Xinhua) -- Lithuanian government approved an initiative on Monday under which online voting could be allowed as soon as in 2016.

The proposal to allow e-voting in Lithuania has been put forward by two ministers of the Lithuanian social-democratic cabinet at a governmental meeting and given green light for the further discussions in the parliament.

But here are Additional Risks!

Non-Technical Risks

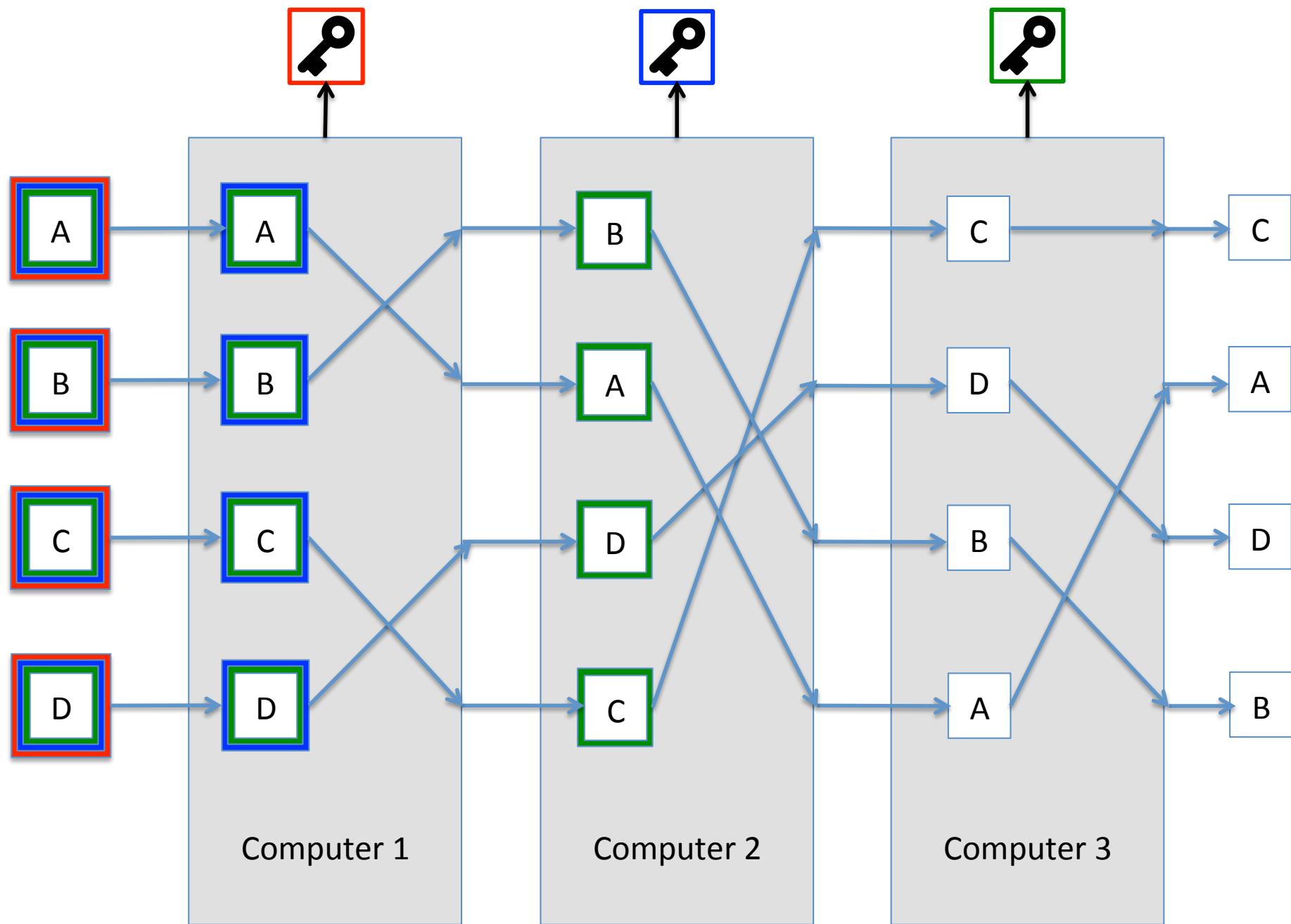
- Hiring election helpers
- Materials
 - Ballots
 - Seals
 - Pens
- Natural disaster
- Resource allocation

Technology induced risks

- Adversaries
 - Honest but curious insider
 - ...
 - Nation State
- Software/hardware bugs
- Single point of failures
- Fall-back procedures
- Key management

What could go wrong?

- Digital ballot forms incorrect [NSW 15]
- No Entropy [Norway 13]
- Configuration problems [Kenya 13]
- Double casting of votes [Geneva 12]
- Voter card printing problem [Norway 11]
- Insecure code [Washington DC 10]



Credible Elections



The Universal Declaration of Human Rights

Article 21. 3.

The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.

Order, Security, Rule of Law



Egypt November 28, 2011

Internet Ballots in Norway



Norway 2013

Verifiability

Properties:

Cast-as-intended

Recorded-as-cast

Counted-as-Recorded

*Cryptographic method:
Zero knowledge proofs*

*Logical method:
Certificates*

*Statistical method:
Risk limiting audits*

Statistical Method

Input: Confidence Level: 99.9%

Party	A	B	C	D	E	F	G	H	I
Seats	5	3		1	1	2	1		0

Audit: Denmark 2014

EU Election: 1903 ballots

Referendum: 60 ballots

Output: Yes/No

```
seed = "90755425186715521560"  
max = 2332217  
for i=1 to samplesize do  
    x = seed ^ "," ^ i  
    y = sha256 (x)  
    z = decimal (y)  
    b = z mod max  
end
```

Conclusion

Electoral Science

- Electoral system innovation
- Internet elections in a post Snowden world
- Education for future generations of experts
- Trust in developing and post-conflict countries
- Trust in established democracies
- Securing digital democracy!

