DEMOCRACY-ENHANCING TECHNOLOGIES

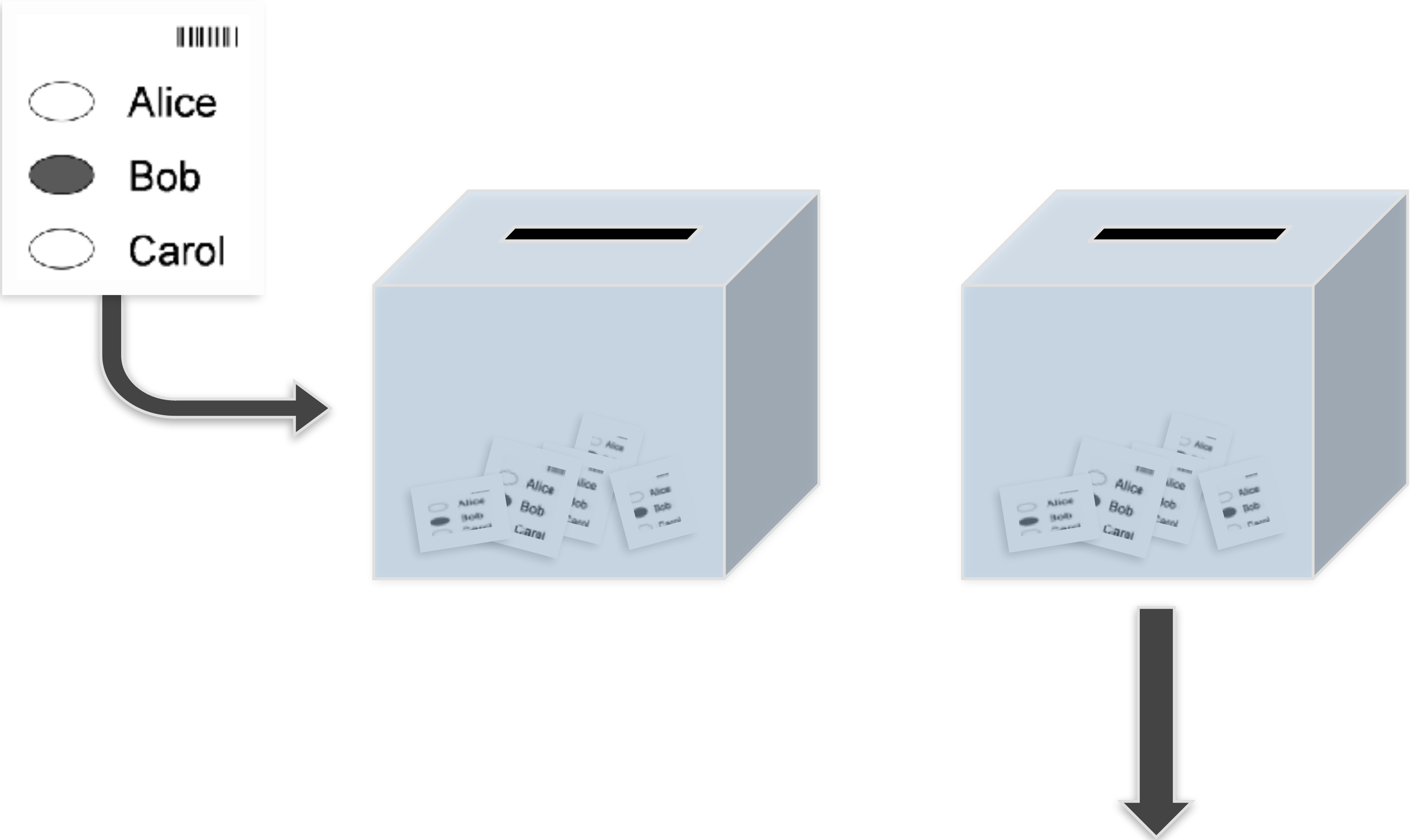
From Theory to Practice

Jeremy Clark

The first election in Canada was a public vote: full integrity but no secrecy

Now we use a secret ballot: secrecy but only weak integrity

Observation allows verification of a single polling place with a full day commitment

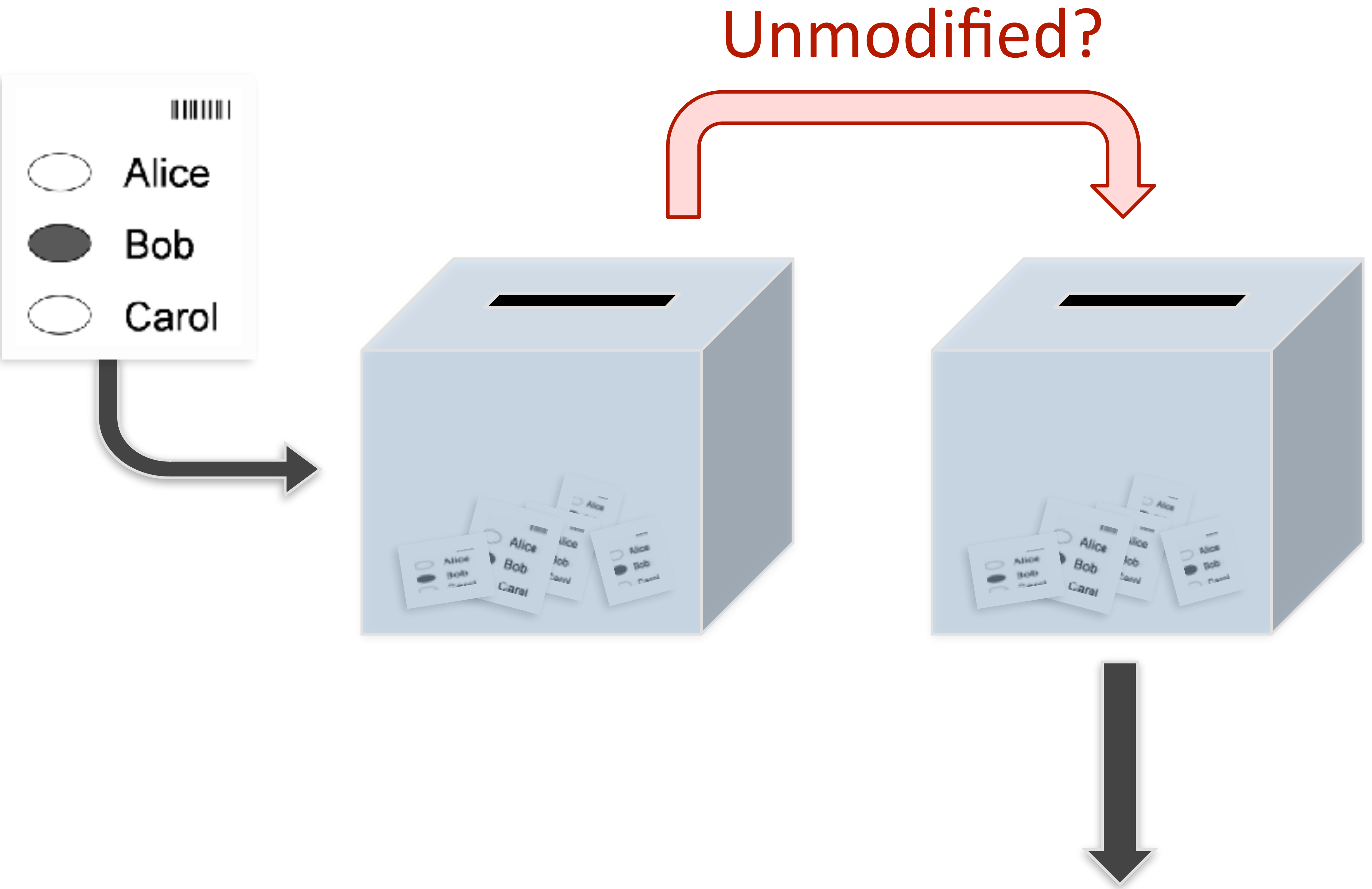


○ Alice

● Bob

○ Carol

Alice	36%
Bob	30%
Carol	34%



Unmodified?

Alice	36%
Bob	30%
Carol	34%

Some municipal elections in Canada use or have used (in-person) electronic voting

Observation is no longer possible

Researchers, when permitted to look, have found the software security is deplorable: the tally is manipulatable under reasonable threat models

End-to-End Verifiable (E2E) Systems offer:

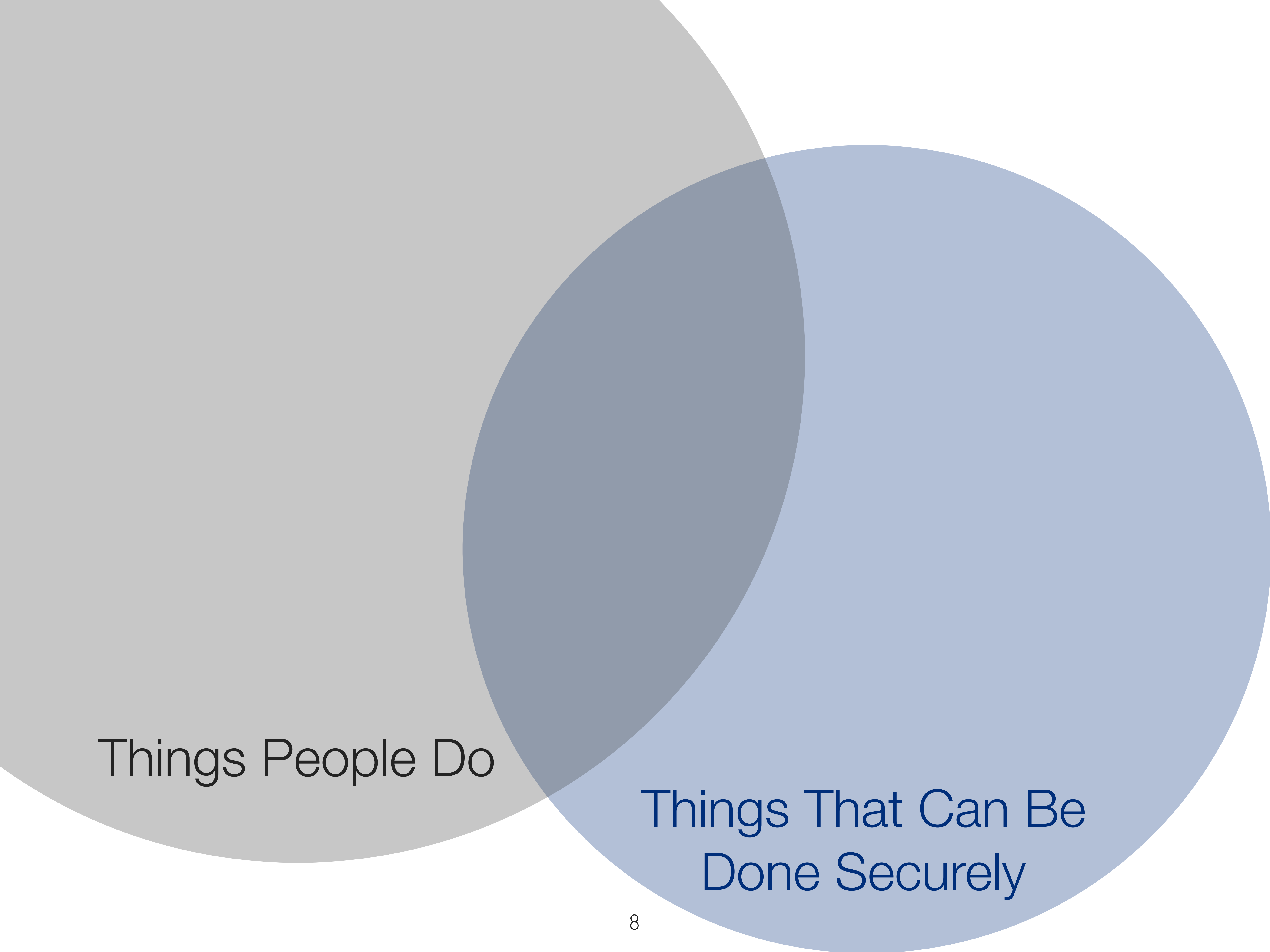
Same integrity as a public vote

Same ballot secrecy as a ballot box

Same level of verification as watching the ballot box all day

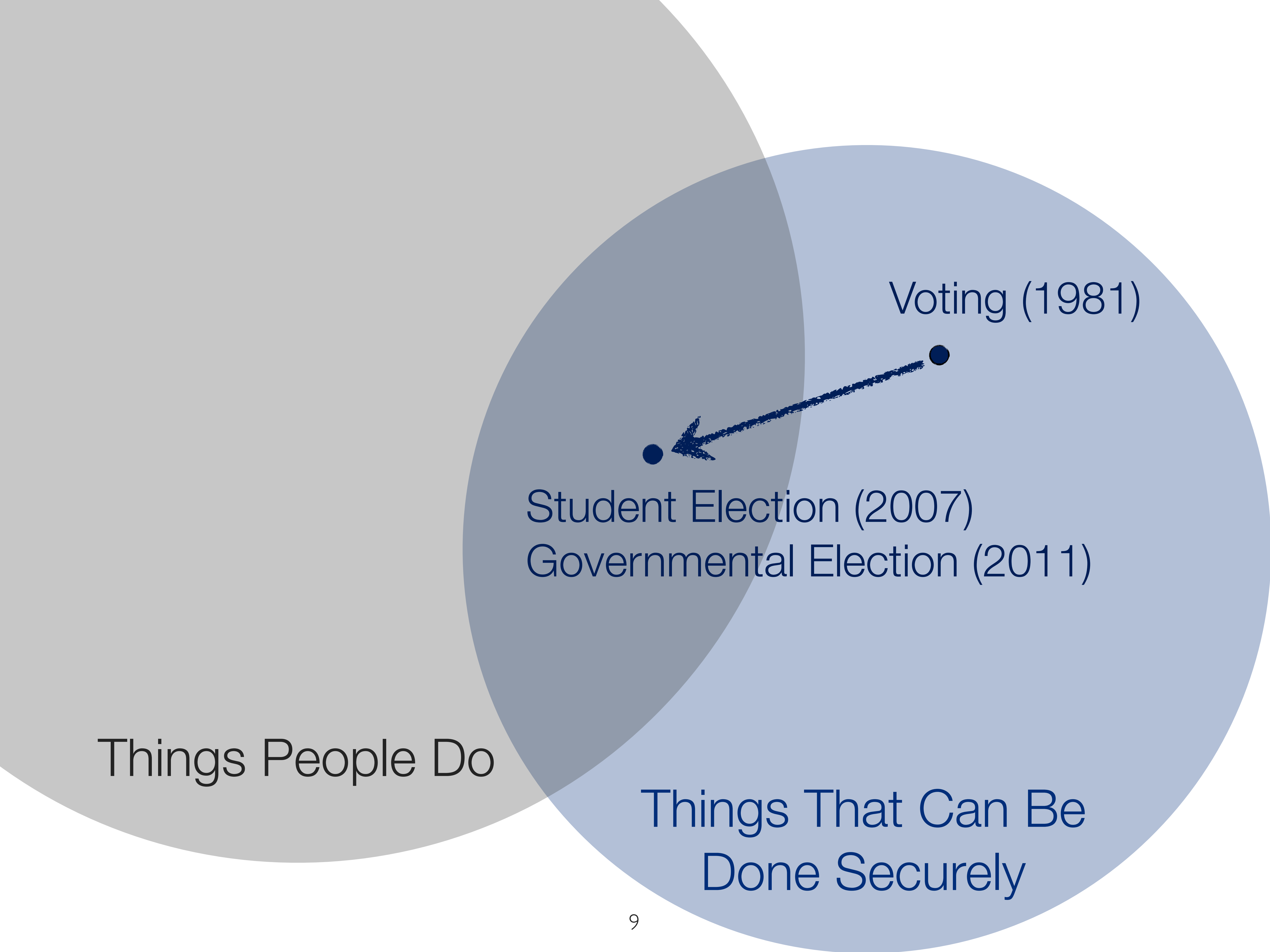
Verification can be done after the election at any time and covers all precincts

Verification soundness is independent of the software



Things People Do

Things That Can Be Done Securely



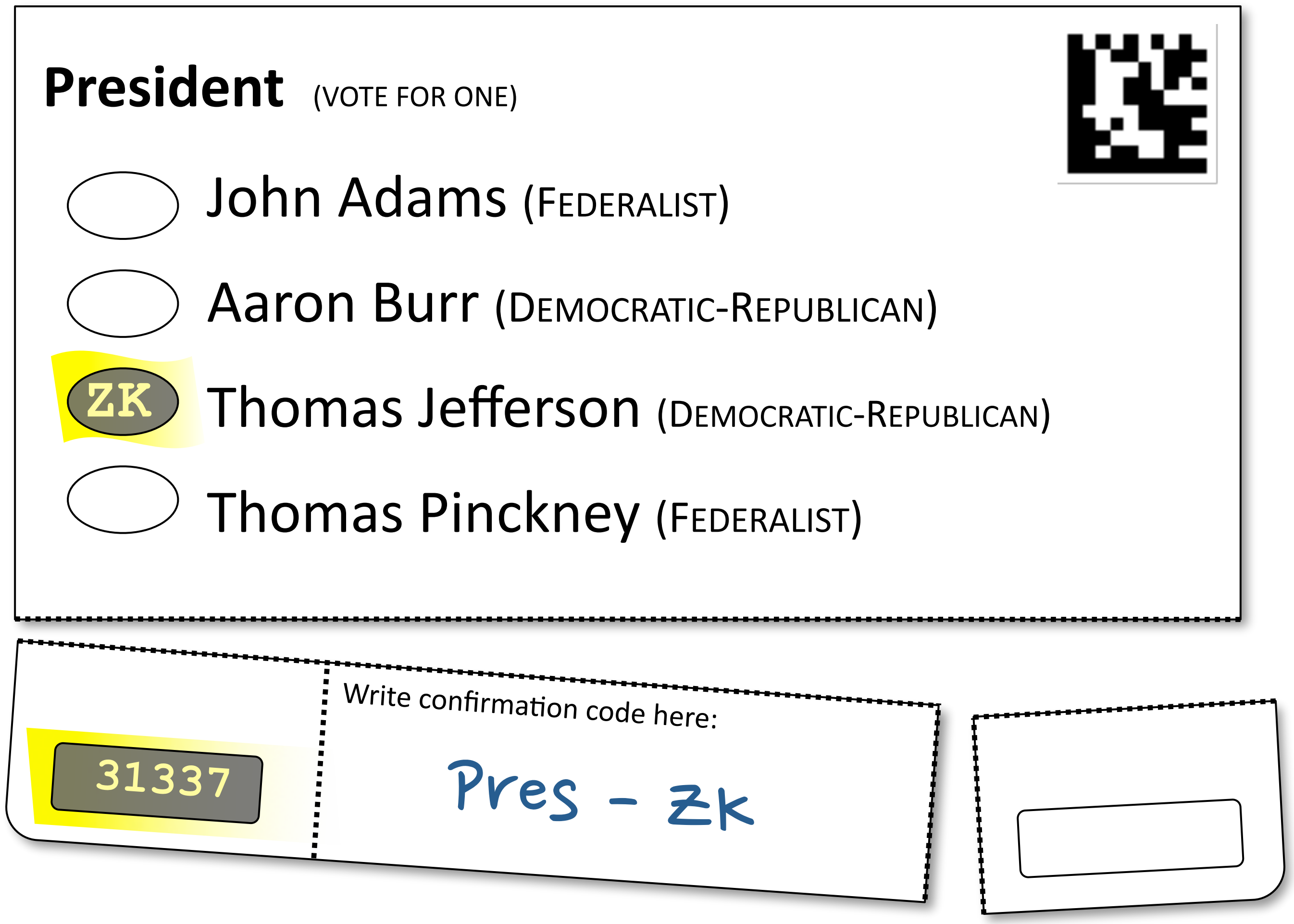
Voting (1981)

Student Election (2007)
Governmental Election (2011)

Things People Do

Things That Can Be
Done Securely

SCANTEGRITY



President (VOTE FOR ONE)

○ John Adams (FEDERALIST)

○ Aaron Burr (DEMOCRATIC-REPUBLICAN)

ZK Thomas Jefferson (DEMOCRATIC-REPUBLICAN)

○ Thomas Pinckney (FEDERALIST)

31337

Write confirmation code here:

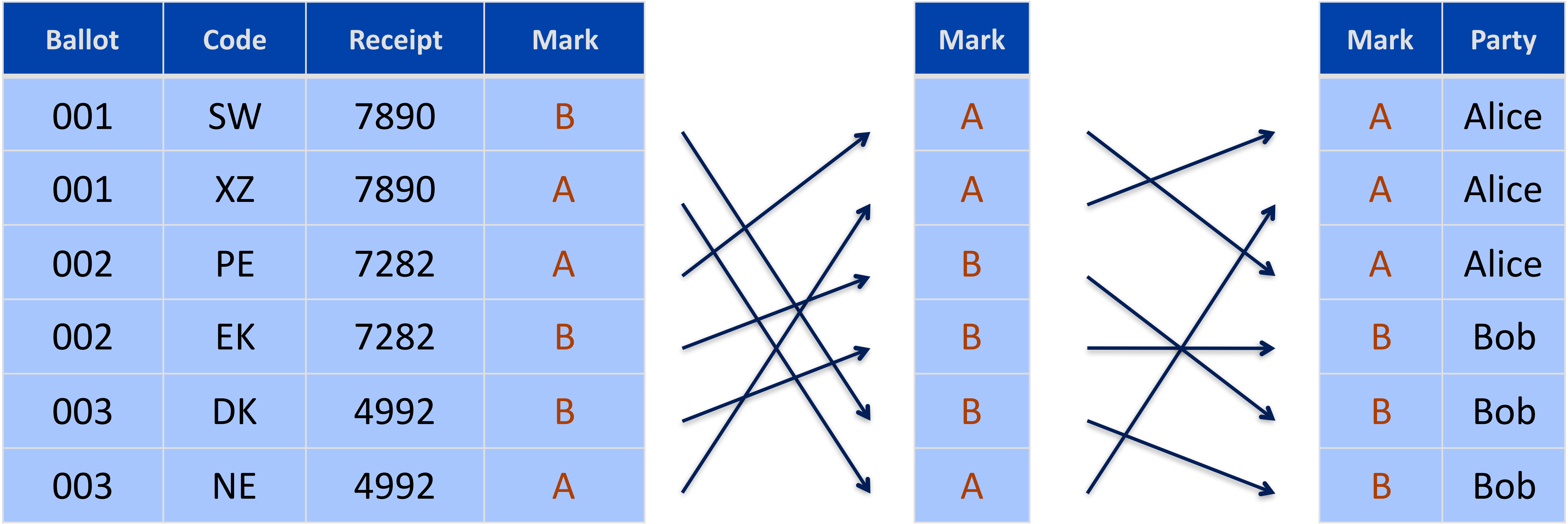
Pres - ZK

UMBC, Waterloo, MIT, GWU

Ballot	Code	Receipt	Mark
001	XZ	7890	
001	SW	7890	
002	PE	7282	
002	EK	7282	
003	NE	4992	
003	DK	4992	

Mark

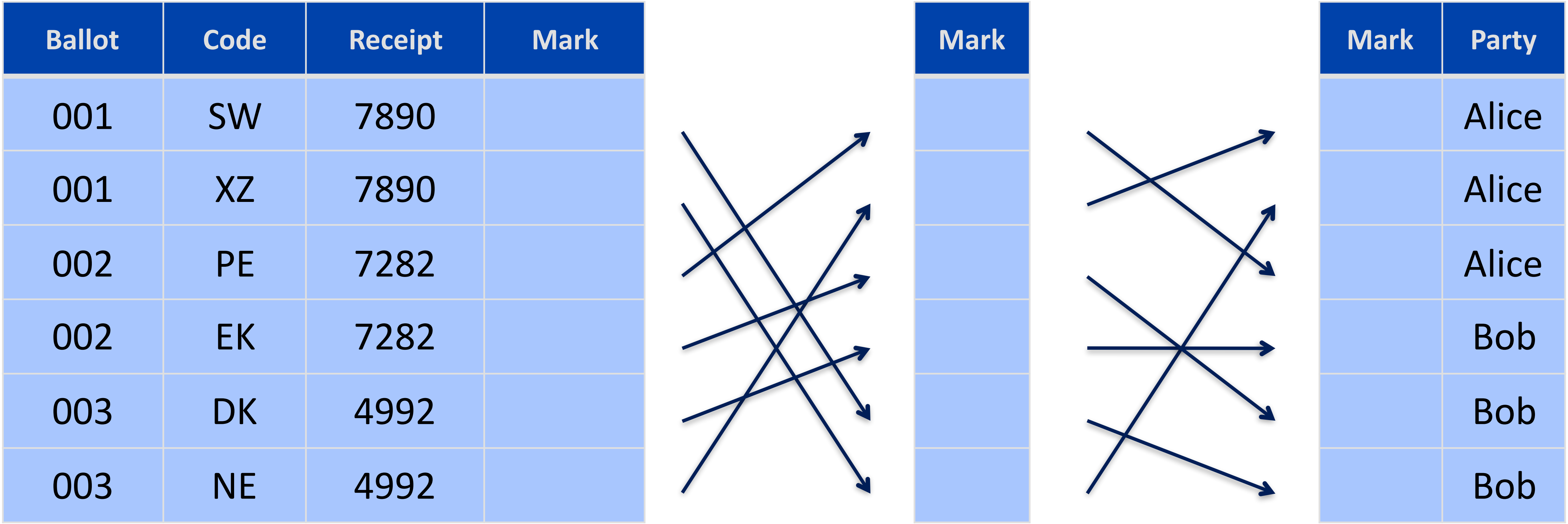
Mark	Party
	Alice
	Bob
	Alice
	Bob
	Alice
	Bob



Ballot	Code	Receipt	Mark
001	SW	7890	B
001	XZ	7890	A
002	PE	7282	A
002	EK	7282	B
003	DK	4992	B
003	NE	4992	A

Mark
A
A
B
B
B
A

Mark	Party
A	Alice
A	Alice
A	Alice
B	Bob
B	Bob
B	Bob

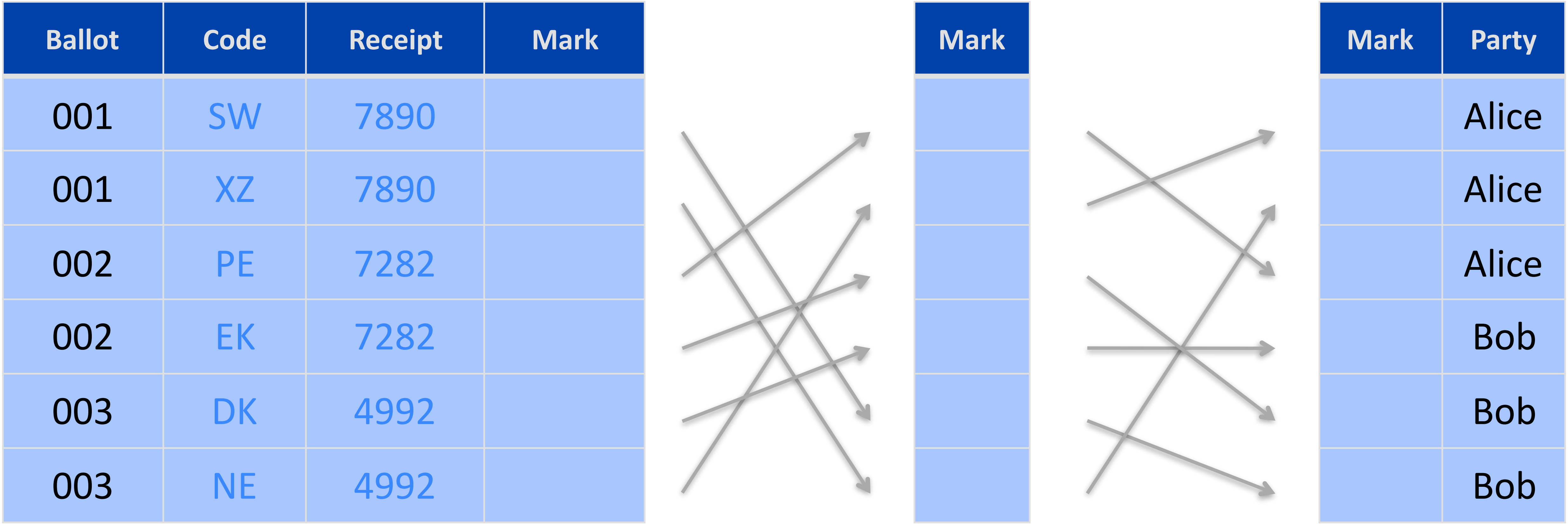


Ballot	Code	Receipt	Mark
001	SW	7890	
001	XZ	7890	
002	PE	7282	
002	EK	7282	
003	DK	4992	
003	NE	4992	

Mark

Mark	Party
	Alice
	Alice
	Alice
	Bob
	Bob
	Bob

Commit to the rows and permutations

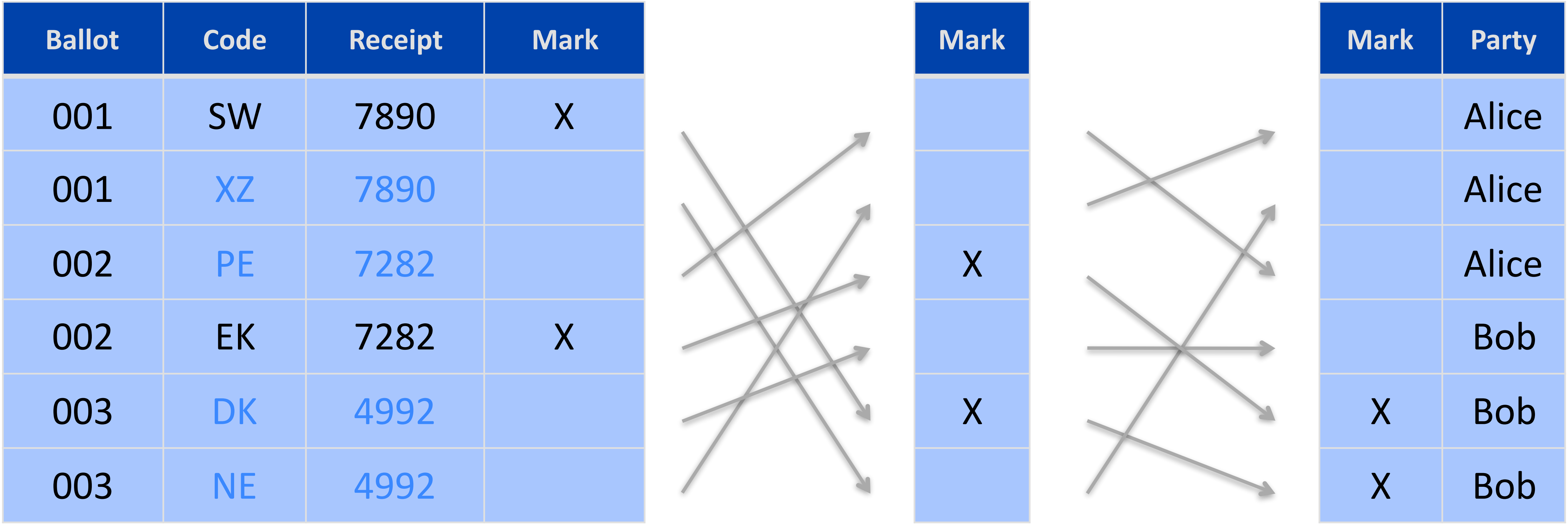


Ballot	Code	Receipt	Mark
001	SW	7890	
001	XZ	7890	
002	PE	7282	
002	EK	7282	
003	DK	4992	
003	NE	4992	

Mark

Mark	Party
	Alice
	Alice
	Alice
	Bob
	Bob
	Bob

Publish tables but not codes or permutations

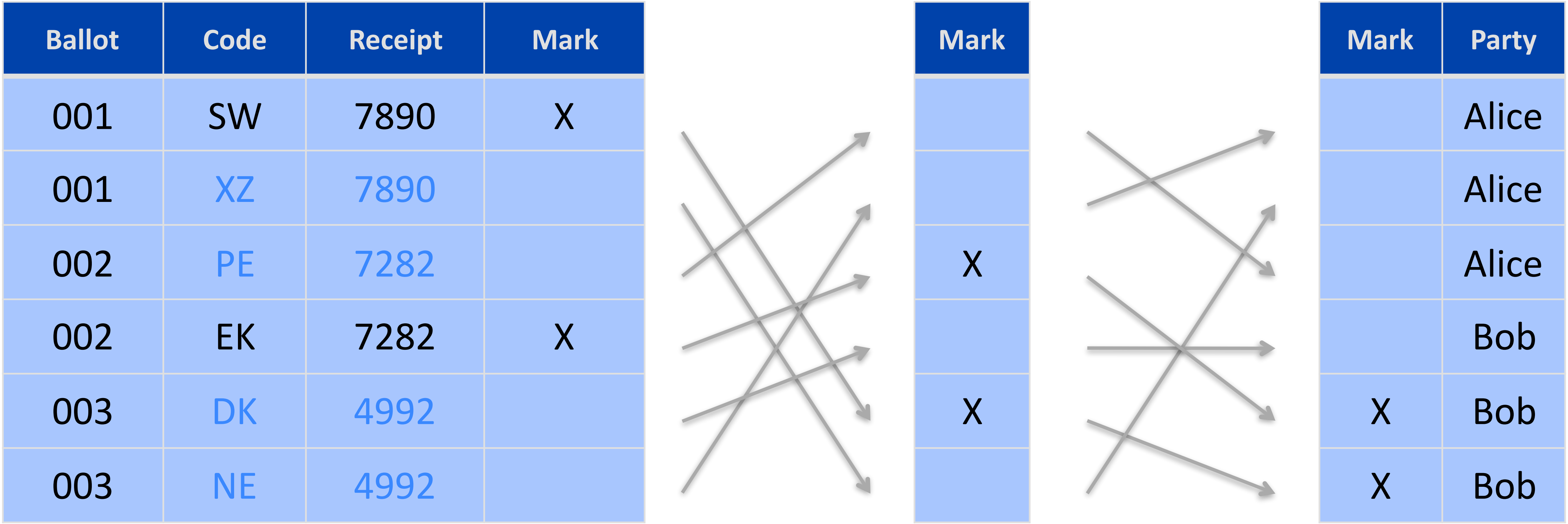


Ballot	Code	Receipt	Mark
001	SW	7890	X
001	XZ	7890	
002	PE	7282	
002	EK	7282	X
003	DK	4992	
003	NE	4992	

Mark
X
X

Mark	Party
	Alice
	Alice
	Alice
	Bob
X	Bob
X	Bob

After voting, fill in table and publish



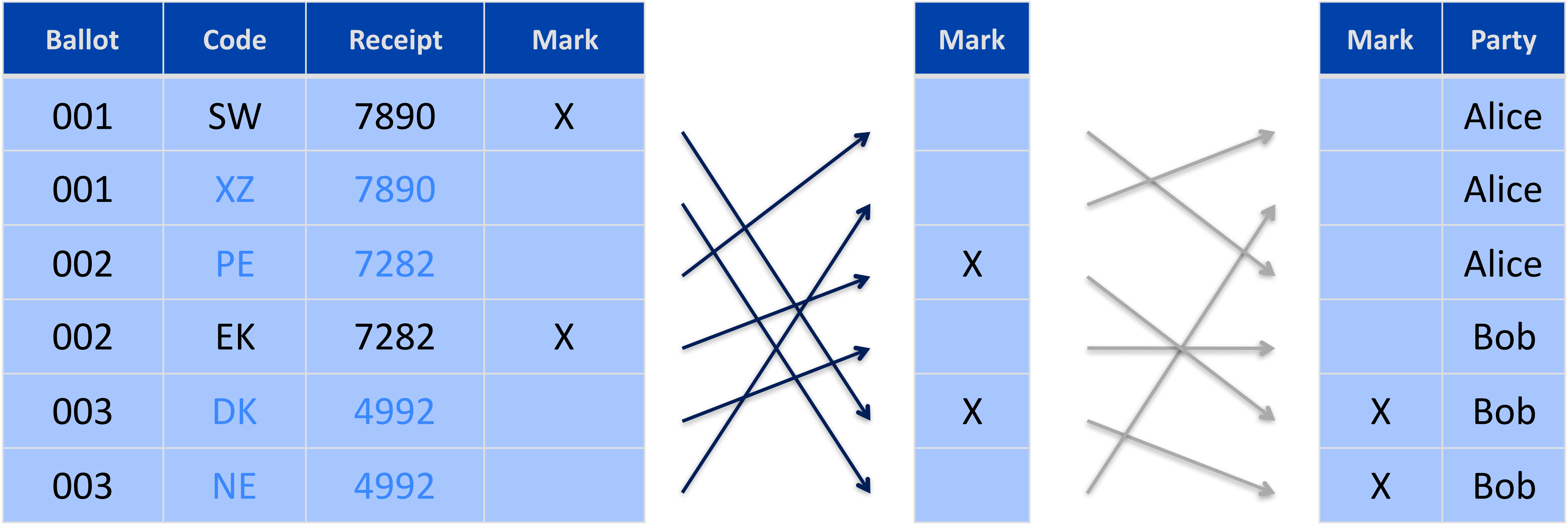
Ballot	Code	Receipt	Mark
001	SW	7890	X
001	XZ	7890	
002	PE	7282	
002	EK	7282	X
003	DK	4992	
003	NE	4992	

Mark
X
X

Mark	Party
	Alice
	Alice
	Alice
	Bob
X	Bob
X	Bob

“Flip a coin” and reveal one of the two permutations

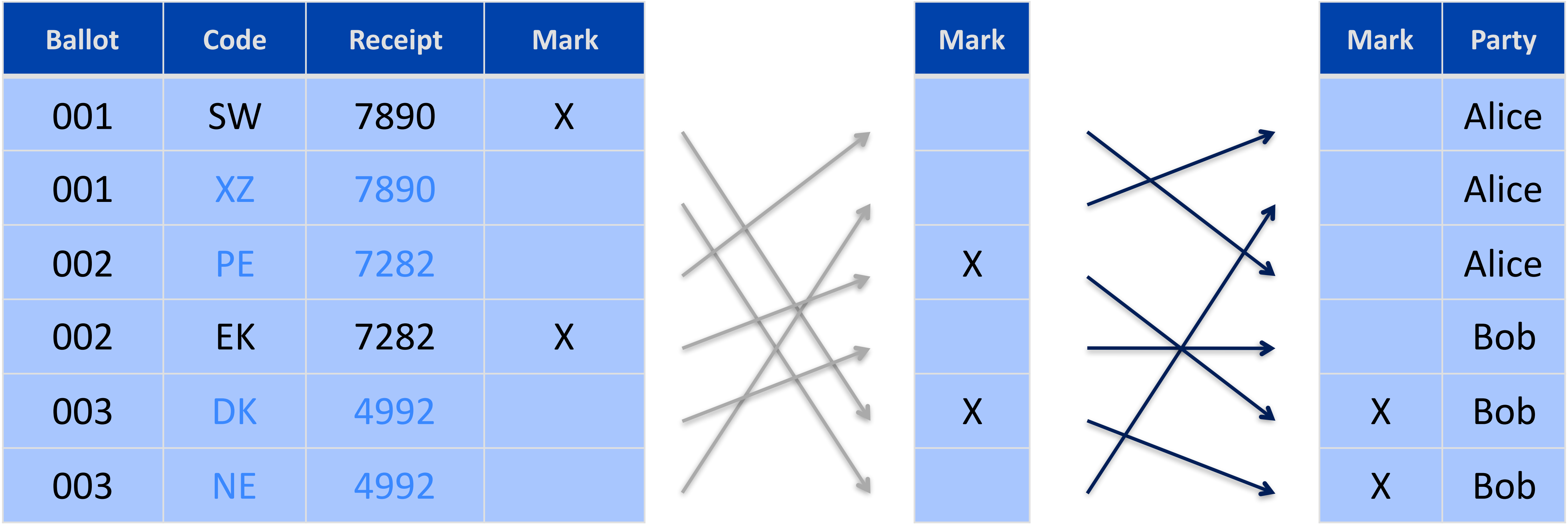
(Closing Price of a DJIA Stock = 6-9 bits of entropy)



Ballot	Code	Receipt	Mark
001	SW	7890	X
001	XZ	7890	
002	PE	7282	
002	EK	7282	X
003	DK	4992	
003	NE	4992	

Mark
X
X

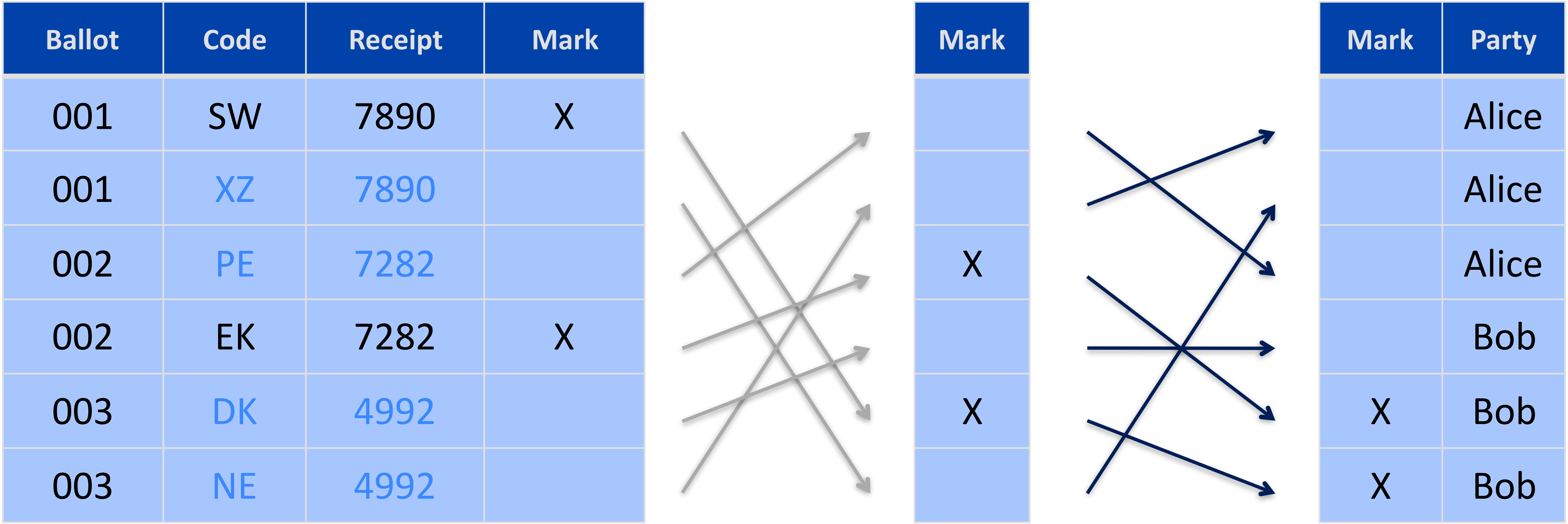
Mark	Party
	Alice
	Alice
	Alice
	Bob
X	Bob
X	Bob



Ballot	Code	Receipt	Mark
001	SW	7890	X
001	XZ	7890	
002	PE	7282	
002	EK	7282	X
003	DK	4992	
003	NE	4992	

Mark
X
X

Mark	Party
	Alice
	Alice
	Alice
	Bob
X	Bob
X	Bob



Ballot	Code	Receipt	Mark
001	SW	7890	X
001	XZ	7890	
002	PE	7282	
002	EK	7282	X
003	DK	4992	
003	NE	4992	

Mark
X
X

Mark	Party
	Alice
	Alice
	Alice
	Bob
X	Bob
X	Bob

Can use many instances.

Cheat detection is: Pr[det] = $(1-1/2^x)$

For example, x=20 gives you >99.9999%

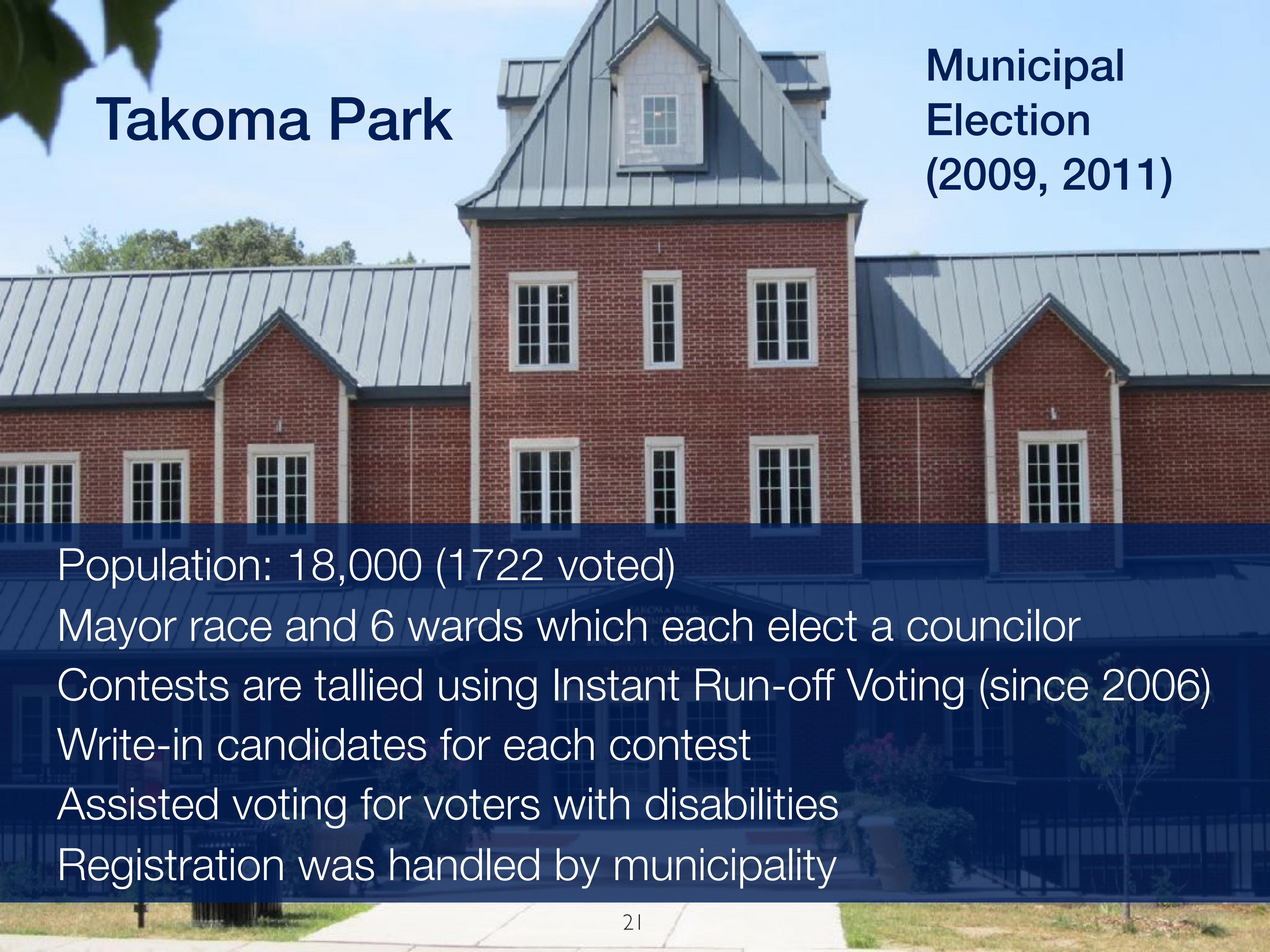
SEE PAPER FOR...

- Dispute Resolution: I wrote down “XY” and the website says “AB”

- Printing Verification: how do you ensure ballots are printed with correct codes?

- Coercion-Resistance: Adversary: “Vote for Alice and wait for my signal to either cast it or spoil it; if spoiled, I’ll make sure you voted for Alice”

- Blackbox Computation: who is computing these tables and how?



Takoma Park

Municipal Election (2009, 2011)

Population: 18,000 (1722 voted)

Mayor race and 6 wards which each elect a councilor

Contests are tallied using Instant Run-off Voting (since 2006)

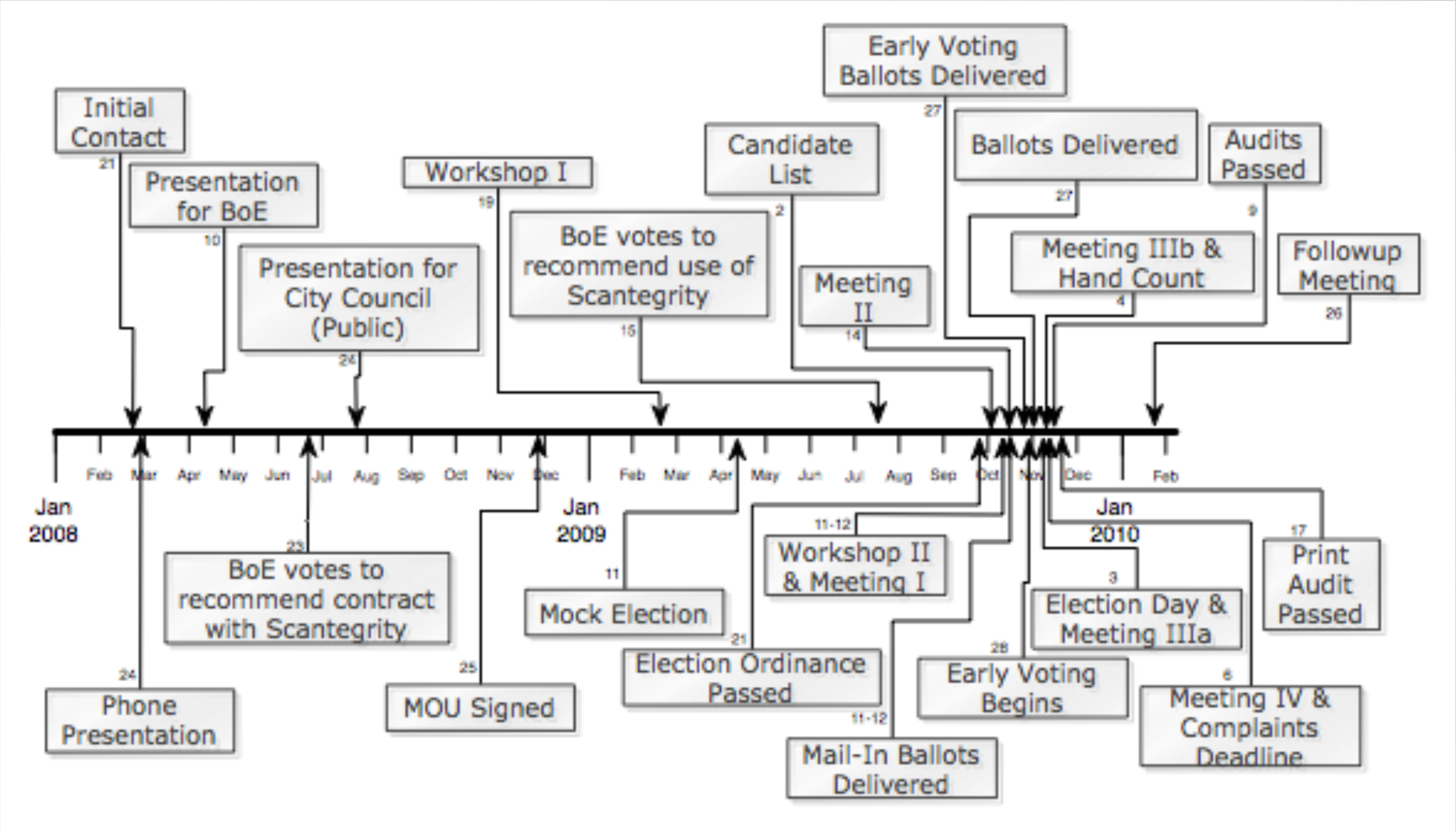
Write-in candidates for each contest

Assisted voting for voters with disabilities

Registration was handled by municipality

Highlights

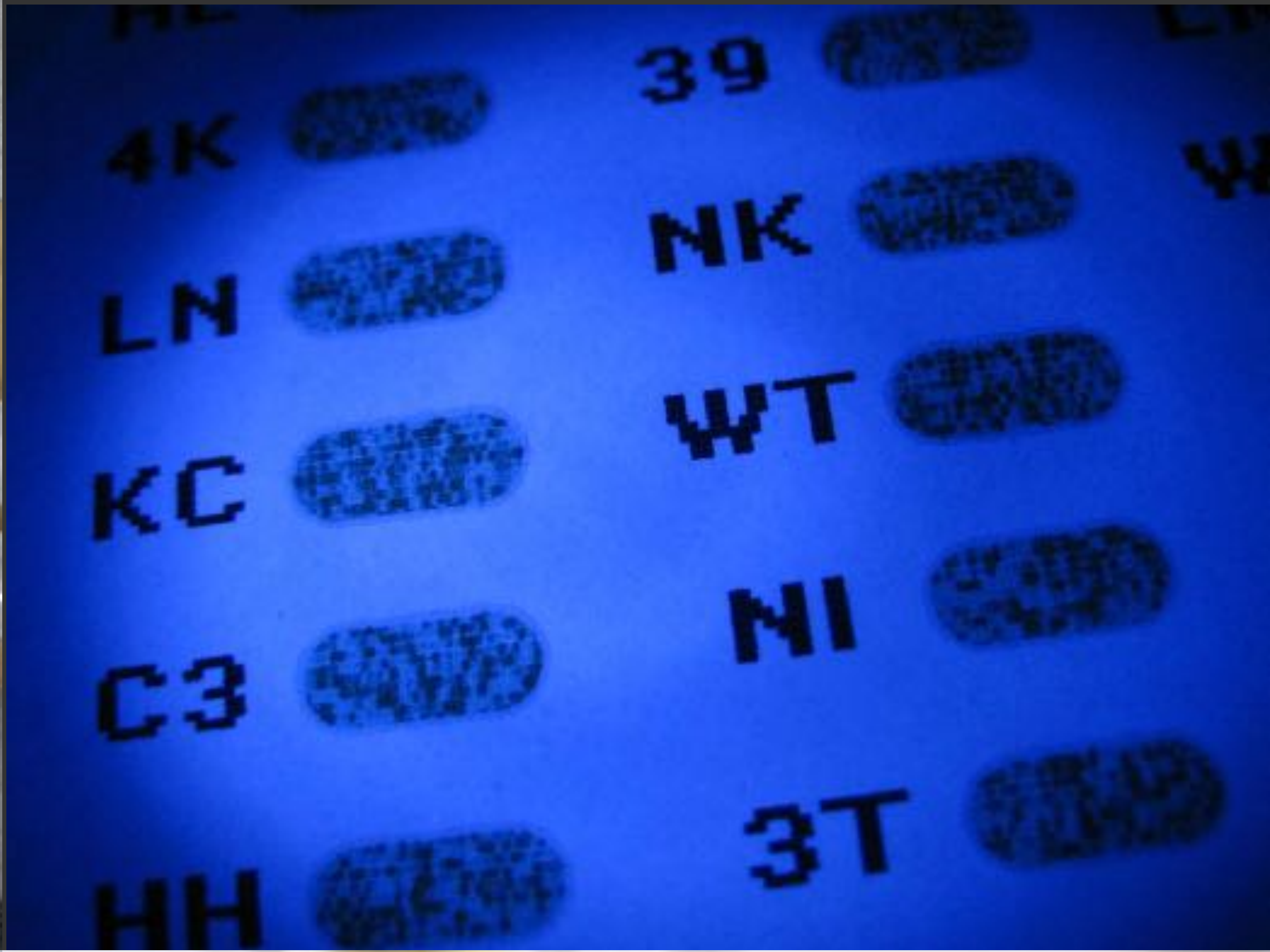
1) Poll worker training and demo of nearly complete system. 8 poll workers and 3 members of the board.

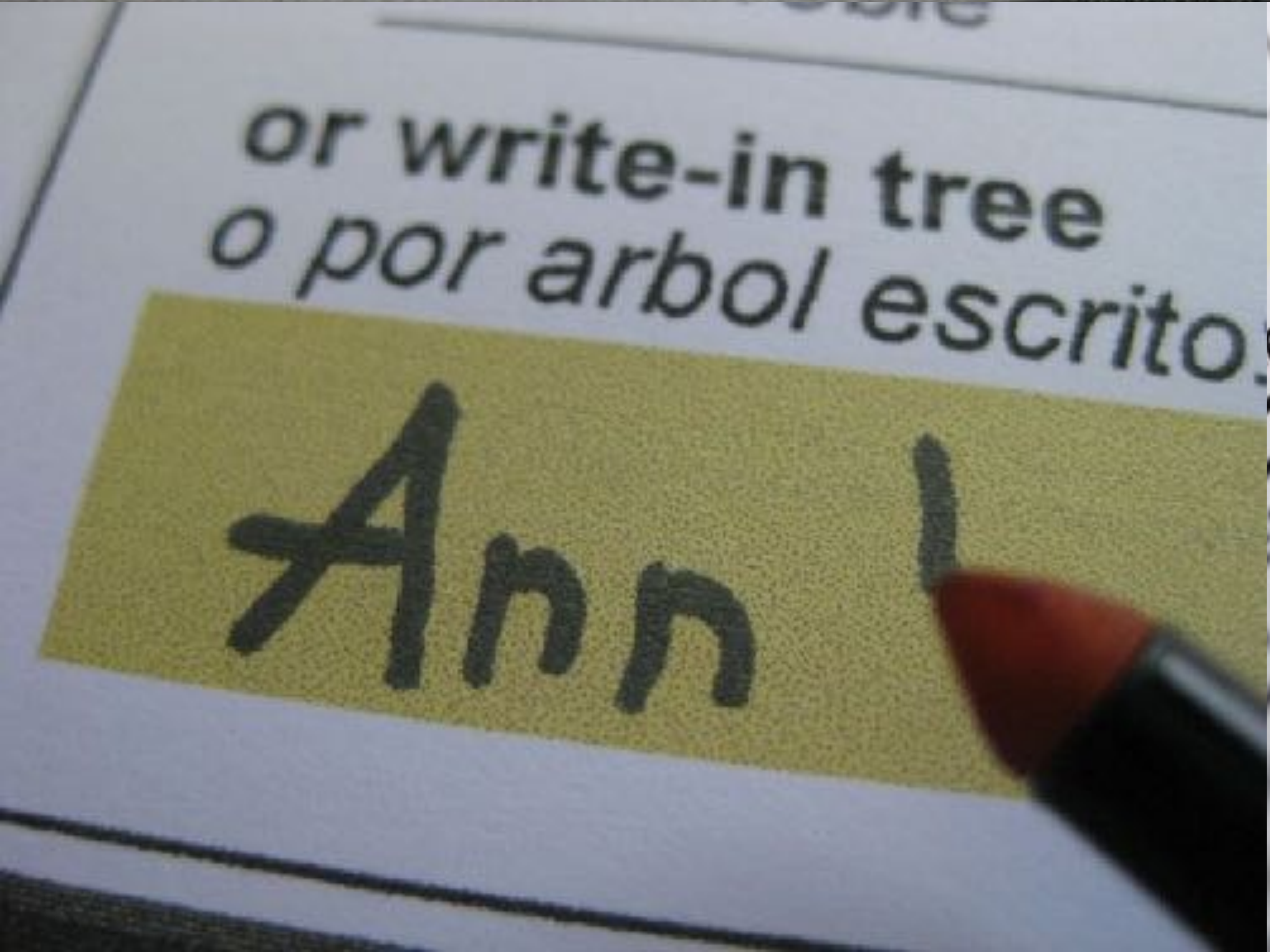


2) Ran a mock election. Collected data:

1. Direct observation (time-to-vote, etc)
2. Voter surveys
3. Poll worker surveys
4. Focus group (with independent interviewer) with voters and poll workers

3) Actual election. Collected data through observation and exit poll surveys (from outside of building)


39
4K
NK
LN
WT
KC
NI
C3
3T
HH

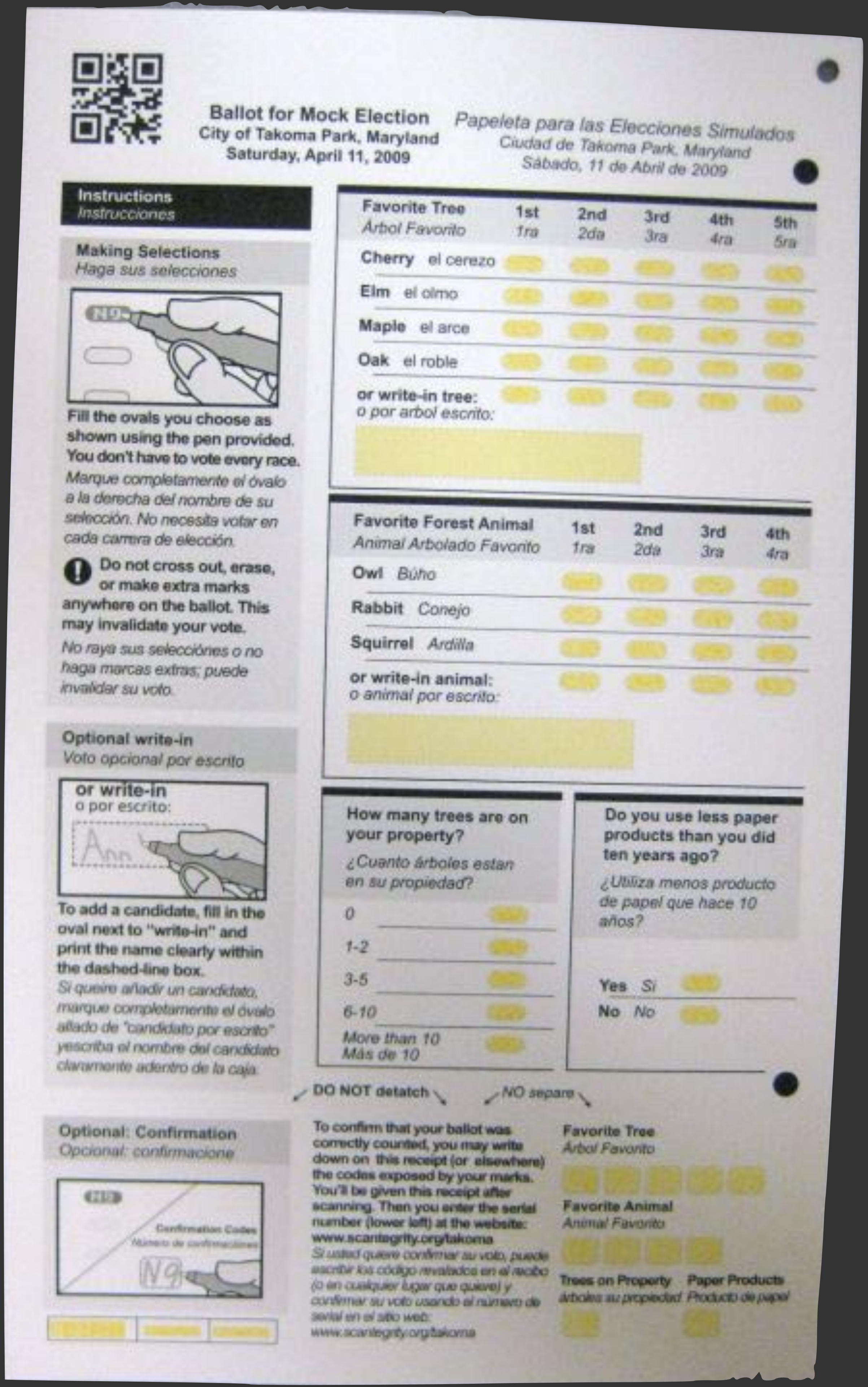

or write-in tree
o por arbol escrito
Ann

ndidato
EMBER WARD 3
CIUDAD DISTRITO ELECTORAL 3
1st choice
1ra opción
2nd choice
2da opción
orden de preferencia

Invisible ink is filtered and injected into ink-jet cartridges for an off-the-shelf CMYK printer

We use four inks: invisible ink, dummy ink, florescent masking ink, and standard black ink

DRM on ink cartridges complicates the process



Ballot for Mock Election
City of Takoma Park, Maryland
Saturday, April 11, 2009

Papeleta para las Elecciones Simulados
Ciudad de Takoma Park, Maryland
Sábado, 11 de Abril de 2009

Instructions
Instrucciones

Making Selections
Haga sus selecciones

Fill the ovals you choose as shown using the pen provided. You don't have to vote every race.
Marque completamente el óvalo a la derecha del nombre de su selección. No necesita votar en cada carrera de elección.

Do not cross out, erase, or make extra marks anywhere on the ballot. This may invalidate your vote.
No raya sus selecciónes o no haga marcas extras; puede invalidar su voto.

Optional write-in
Voto opcional por escrito

To add a candidate, fill in the oval next to "write-in" and print the name clearly within the dashed-line box.
Si queire añadir un candidato, marque completamente el óvalo alado de "candidato por escrito" yescriba el nombre del candidato claramente adentro de la caja.

Favorite Tree *Árbol Favorito*	1st *1ra*	2nd *2da*	3rd *3ra*	4th *4ra*	5th *5ra*
Cherry el cerezo	○	○	○	○	○
Elm el olmo	○	○	○	○	○
Maple el arce	○	○	○	○	○
Oak el roble	○	○	○	○	○
or write-in tree: *o por arbol escrito:*	○	○	○	○	○

Favorite Forest Animal *Animal Arbolado Favorito*	1st *1ra*	2nd *2da*	3rd *3ra*	4th *4ra*
Owl *Búho*	○	○	○	○
Rabbit *Conejo*	○	○	○	○
Squirrel *Ardilla*	○	○	○	○
or write-in animal: *o animal por escrito:*	○	○	○	○

How many trees are on your property?
¿Cuanto árboles estan en su propiedad?

0	○
1-2	○
3-5	○
6-10	○
More than 10 *Más de 10*	○

Do you use less paper products than you did ten years ago?
¿Utiliza menos producto de papel que hace 10 años?

Yes *Si*	○
No *No*	○

DO NOT detatch *NO separe*

Optional: Confirmation
Opcional: confirmacione

To confirm that your ballot was correctly counted, you may write down on this receipt (or elsewhere) the codes exposed by your marks. You'll be given this receipt after scanning. Then you enter the serial number (lower left) at the website: www.scantegrity.org/takoma
Si usted quiere confirmar su voto, puede escribir los código revelados en el recibo (o en cualquier lugar que quiere) y confirmar su voto usando el número de serial en el sitio web: www.scantegrity.org/takoma

Favorite Tree
Árbol Favorito

Favorite Animal
Animal Favorito

Trees on Property
árboles su propiedad

Paper Products
Producto de papel

Design for Democracy

(AIGA)

Marcia Lausen

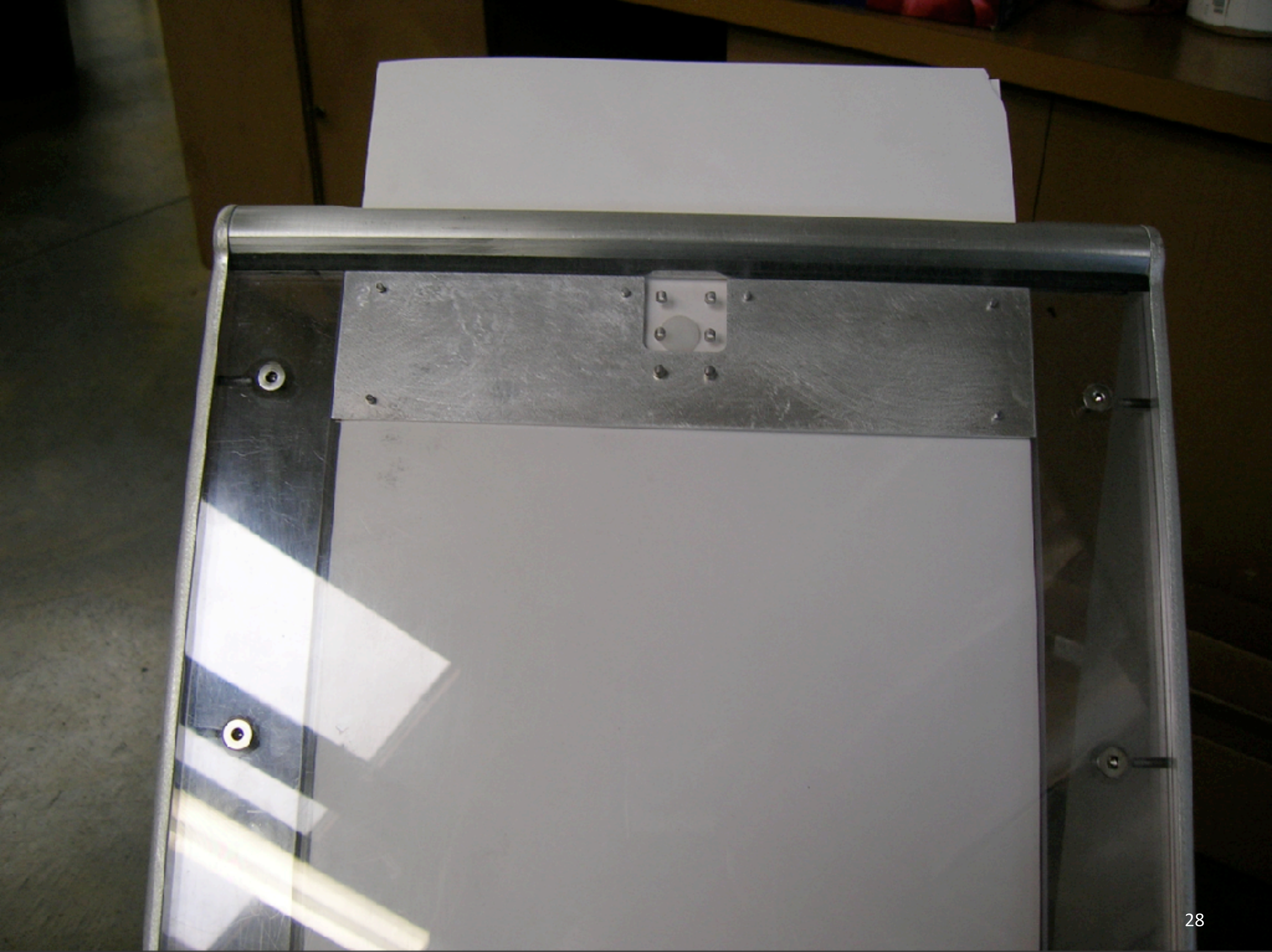
IMPROVEMENTS (MOCK)

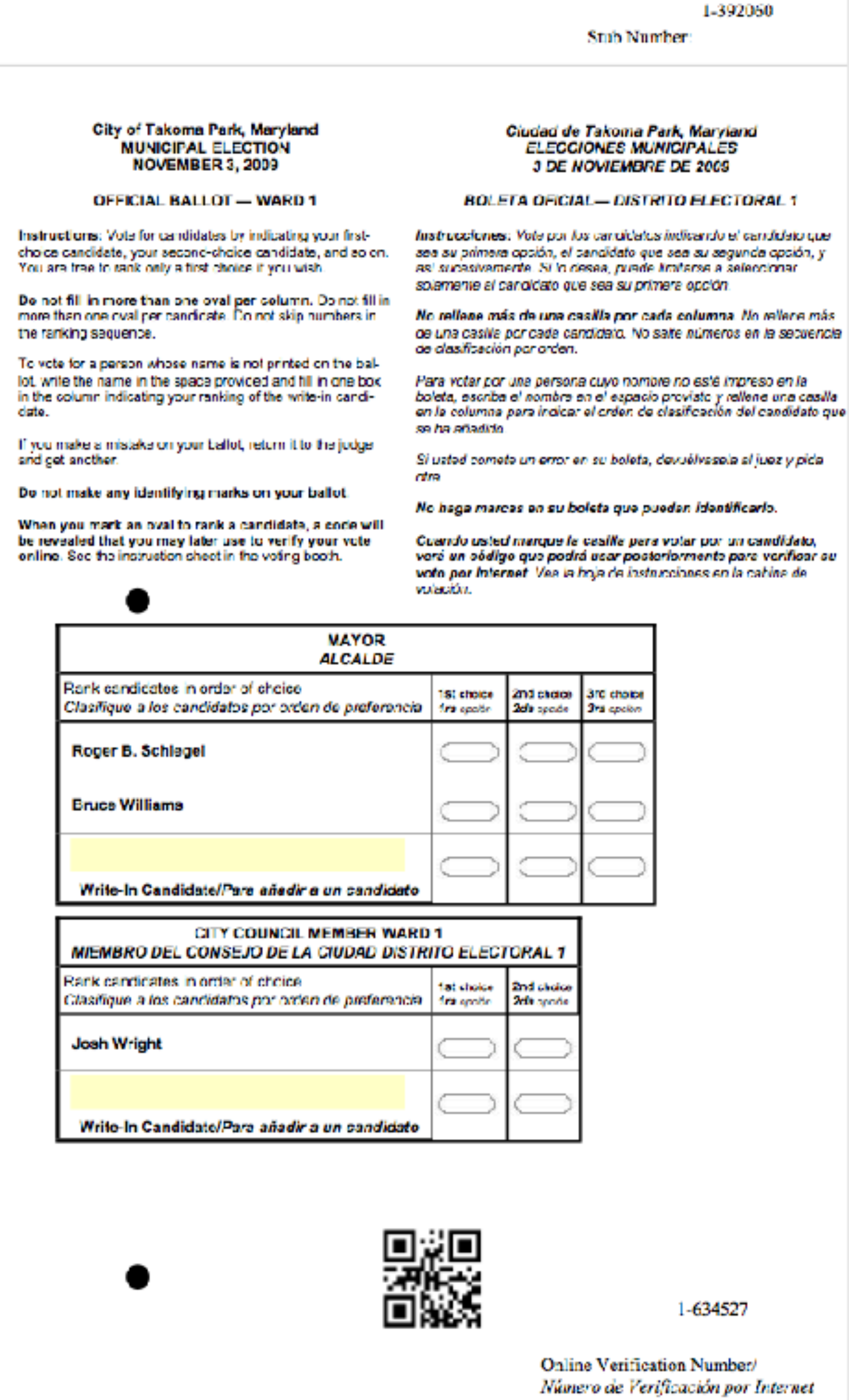
Improved the pens (less smudging, two tips)

Simplified ballot casting process (no locks, no intervention from poll worker during casting, direct feed into scanner)

Separate verification card

Confirmation codes were switched to three digits (from a two-character reduced set)





1-392060

Stub Number

City of Takoma Park, Maryland
MUNICIPAL ELECTION
NOVEMBER 3, 2009

OFFICIAL BALLOT — WARD 1

Instructions: Vote for candidates by indicating your first-choice candidate, your second-choice candidate, and so on. You are free to rank only a first choice if you wish.

Do not fill in more than one oval per column. Do not fill in more than one oval per candidate. Do not skip numbers in the ranking sequence.

To vote for a person whose name is not printed on the ballot, write the name in the space provided and fill in one box in the column indicating your ranking of the write-in candidate.

If you make a mistake on your ballot, return it to the judge and get another.

Do not make any identifying marks on your ballot.

When you mark an oval to rank a candidate, a code will be revealed that you may later use to verify your vote online. See the instruction sheet in the voting booth.

Ciudad de Takoma Park, Maryland
ELECCIONES MUNICIPALES
3 DE NOVIEMBRE DE 2009

BOLETA OFICIAL — DISTRITO ELECTORAL 1

Instrucciones: *Vote por los candidatos indicando el candidato que sea su primera opción, el candidato que sea su segunda opción, y así sucesivamente. Si lo desea, puede limitarse a seleccionar solamente el candidato que sea su primera opción.*

No rellene más de una casilla por cada columna. *No rellene más de una casilla por cada candidato. No salte números en la secuencia de clasificación por orden.*

Para votar por una persona cuyo nombre no esté impreso en la boleta, escriba el nombre en el espacio previsto y rellene una casilla en la columna para indicar el orden de clasificación del candidato que se ha añadido.

Si usted comete un error en su boleta, devuélvasela al juez y pida otra.

No haga marcas en su boleta que puedan identificarlo.

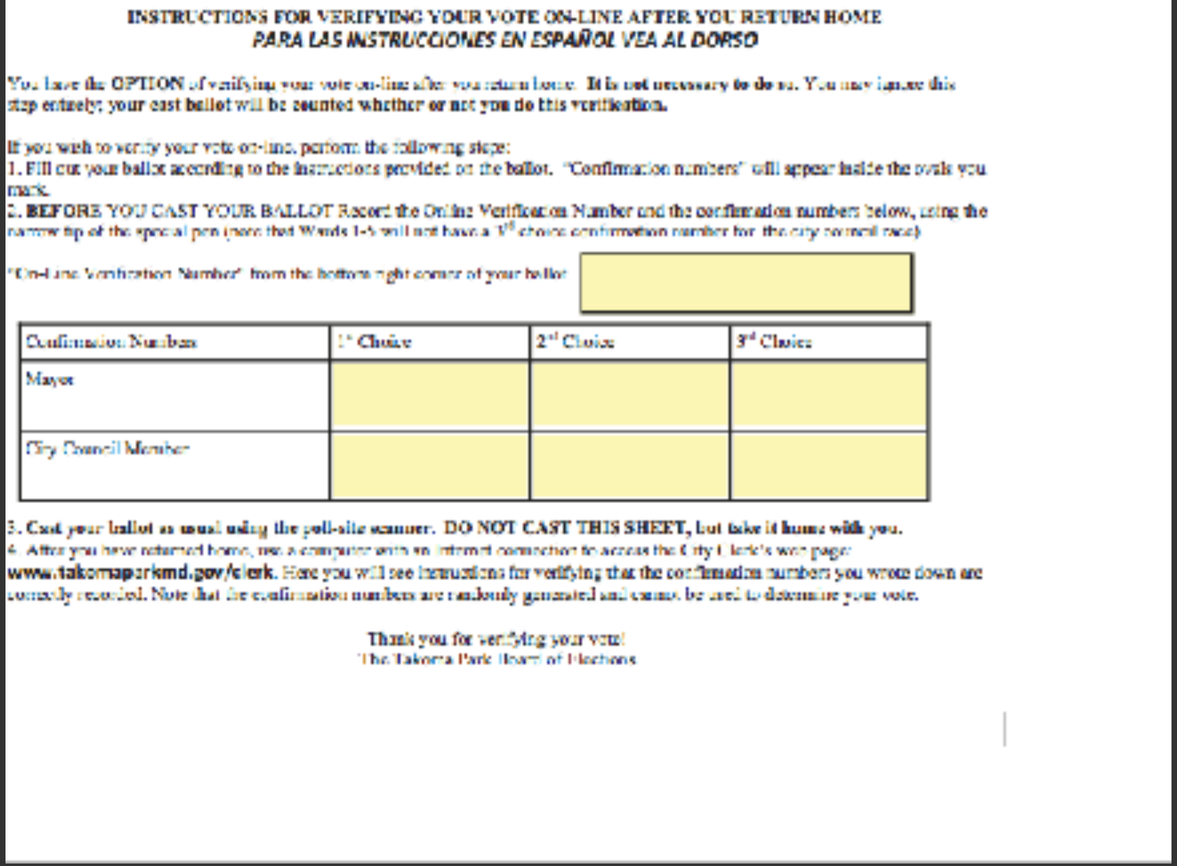
Cuando usted marque la casilla para votar por un candidato, verá un código que podrá usar posteriormente para verificar su voto por Internet. *Vea la hoja de instrucciones en la cabina de votación.*

MAYOR *ALCALDE*			
Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	1st choice *1ra opción*	2nd choice *2da opción*	3rd choice *3ra opción*
Roger B. Schlegel	○	○	○
Bruce Williams	○	○	○
Write-In Candidate/*Para añadir a un candidato*	○	○	○

CITY COUNCIL MEMBER WARD 1 *MIEMBRO DEL CONSEJO DE LA CIUDAD DISTRITO ELECTORAL 1*		
Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	1st choice *1ra opción*	2nd choice *2da opción*
Josh Wright	○	○
Write-In Candidate/*Para añadir a un candidato*	○	○

1-634527

Online Verification Number/
Número de Verificación por Internet



INSTRUCTIONS FOR VERIFYING YOUR VOTE ON-LINE AFTER YOU RETURN HOME
PARA LAS INSTRUCCIONES EN ESPAÑOL VEA AL DORSO

You have the OPTION of verifying your vote on-line after you return home. **It is not necessary to do so.** You may ignore this step entirely; **your cast ballot will be counted whether or not you do this verification.**

If you wish to verify your vote on-line, perform the following steps:

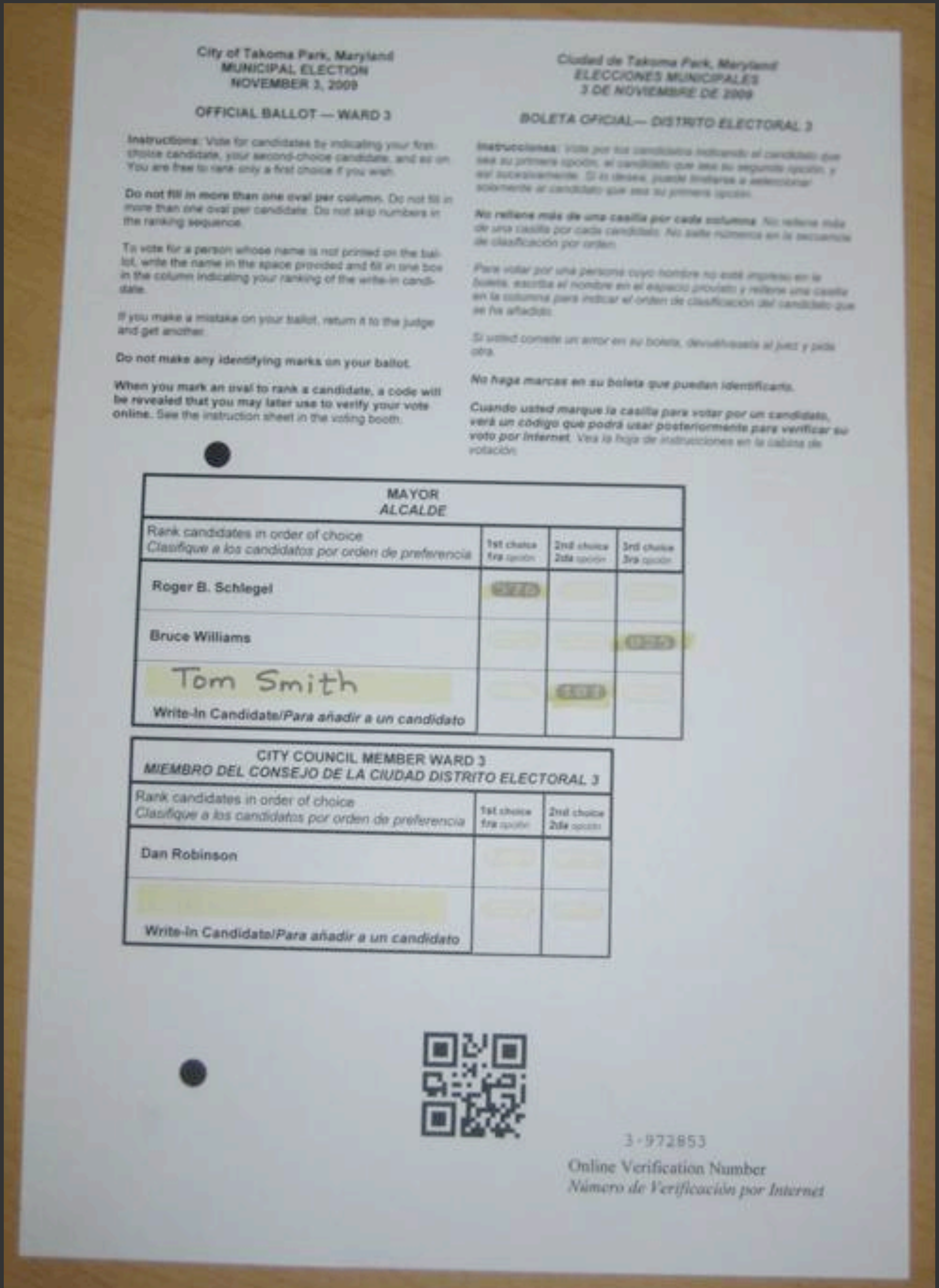
1. Fill out your ballot according to the instructions provided on the ballot. "Confirmation numbers" will appear inside the ovals you mark.
2. **BEFORE YOU CAST YOUR BALLOT** Record the Online Verification Number and the confirmation numbers below, using the narrow tip of the special pen (note that Wards 1-5 will not have a 3rd choice confirmation number for the city council race)

"On-Line Verification Number" from the bottom right corner of your ballot:

Confirmation Numbers	1st Choice	2nd Choice	3rd Choice
Mayor			
City Council Member			

3. **Cast your ballot as usual using the poll-site scanner. DO NOT CAST THIS SHEET, but take it home with you.**
4. After you have returned home, use a computer with an Internet connection to access the City Clerk's web page: **www.takomaparkmd.gov/clerk**. Here you will see instructions for verifying that the confirmation numbers you wrote down are correctly recorded. Note that the confirmation numbers are randomly generated and cannot be used to determine your vote.

Thank you for verifying your vote!
The Takoma Park Board of Elections



City of Takoma Park, Maryland
MUNICIPAL ELECTION
NOVEMBER 3, 2009

OFFICIAL BALLOT — WARD 3

Instructions: Vote for candidates by indicating your first-choice candidate, your second-choice candidate, and so on. You are free to rank only a first choice if you wish.

Do not fill in more than one oval per column. Do not fill in more than one oval per candidate. Do not skip numbers in the ranking sequence.

To vote for a person whose name is not printed on the ballot, write the name in the space provided and fill in one box in the column indicating your ranking of the write-in candidate.

If you make a mistake on your ballot, return it to the judge and get another.

Do not make any identifying marks on your ballot.

When you mark an oval to rank a candidate, a code will be revealed that you may later use to verify your vote online. See the instruction sheet in the voting booth.

Ciudad de Takoma Park, Maryland
ELECCIONES MUNICIPALES
3 DE NOVIEMBRE DE 2009

BOLETA OFICIAL— DISTRITO ELECTORAL 3

Instrucciones: *Vote por los candidatos indicando el candidato que sea su primera opción, el candidato que sea su segunda opción, y así sucesivamente. Si lo desea, puede limitarse a seleccionar solamente al candidato que sea su primera opción.*

No rellene más de una casilla por cada columna. *No rellene más de una casilla por cada candidato. No salte números en la secuencia de clasificación por orden.*

Para votar por una persona cuyo nombre no está impreso en la boleta, escriba el nombre en el espacio provisto y rellene una casilla en la columna para indicar el orden de clasificación del candidato que se ha añadido.

Si usted comete un error en su boleta, devuélvasela al juez y pida otra.

No haga marcas en su boleta que puedan identificarlo.

Cuando usted marque la casilla para votar por un candidato, verá un código que podrá usar posteriormente para verificar su voto por Internet. *Vea la hoja de instrucciones en la cabina de votación.*

MAYOR
ALCALDE

Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	1st choice 1ra opción	2nd choice 2da opción	3rd choice 3ra opción
Roger B. Schlegel	[illegible]		
Bruce Williams			[illegible]
Tom Smith **Write-In Candidate/*Para añadir a un candidato***		[illegible]	

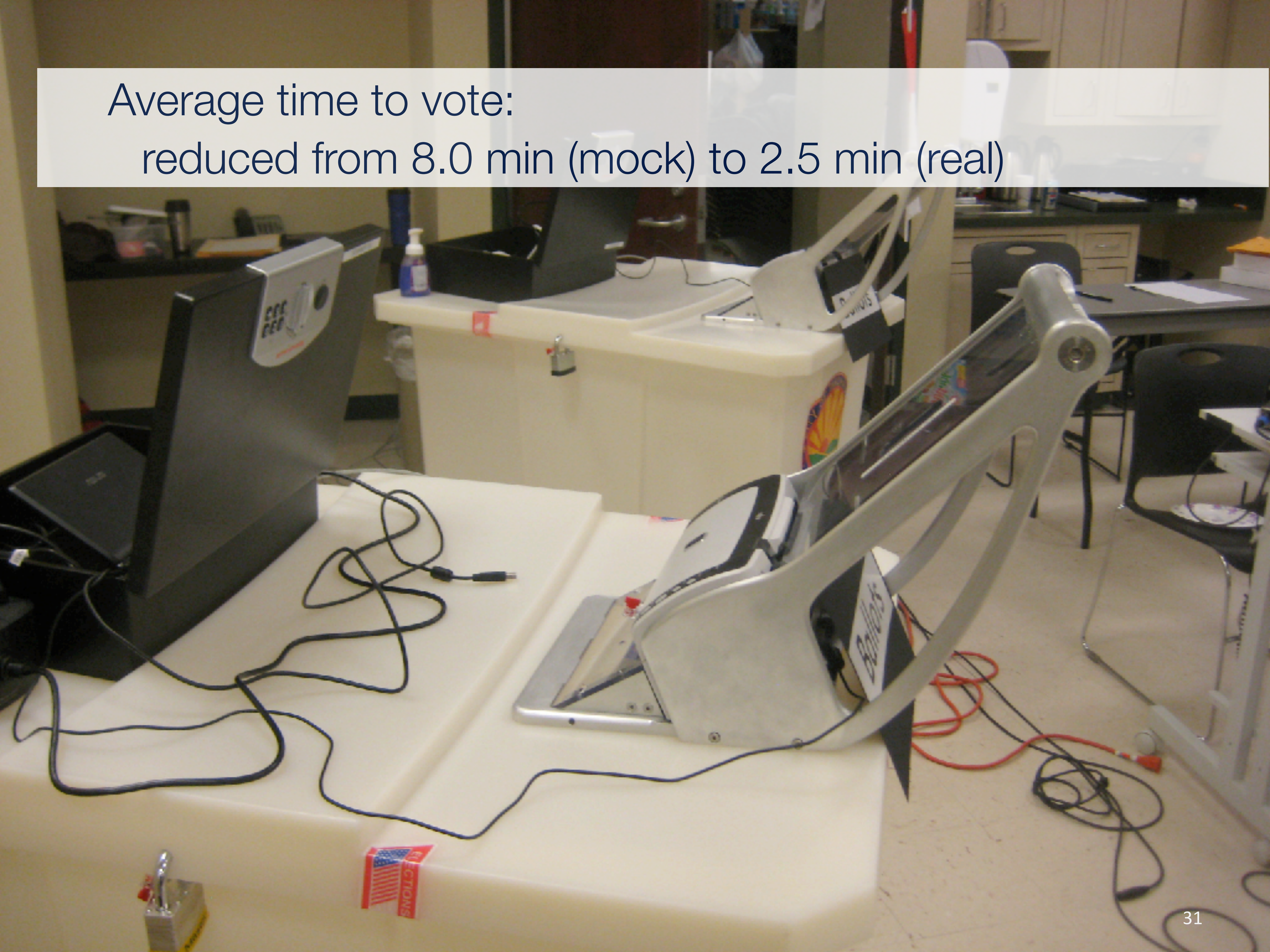
CITY COUNCIL MEMBER WARD 3
MIEMBRO DEL CONSEJO DE LA CIUDAD DISTRITO ELECTORAL 3

Rank candidates in order of choice *Clasifique a los candidatos por orden de preferencia*	1st choice 1ra opción	2nd choice 2da opción
Dan Robinson		
Write-In Candidate/*Para añadir a un candidato*		

3-972853
Online Verification Number
Número de Verificación por Internet

Average time to vote:

reduced from 8.0 min (mock) to 2.5 min (real)



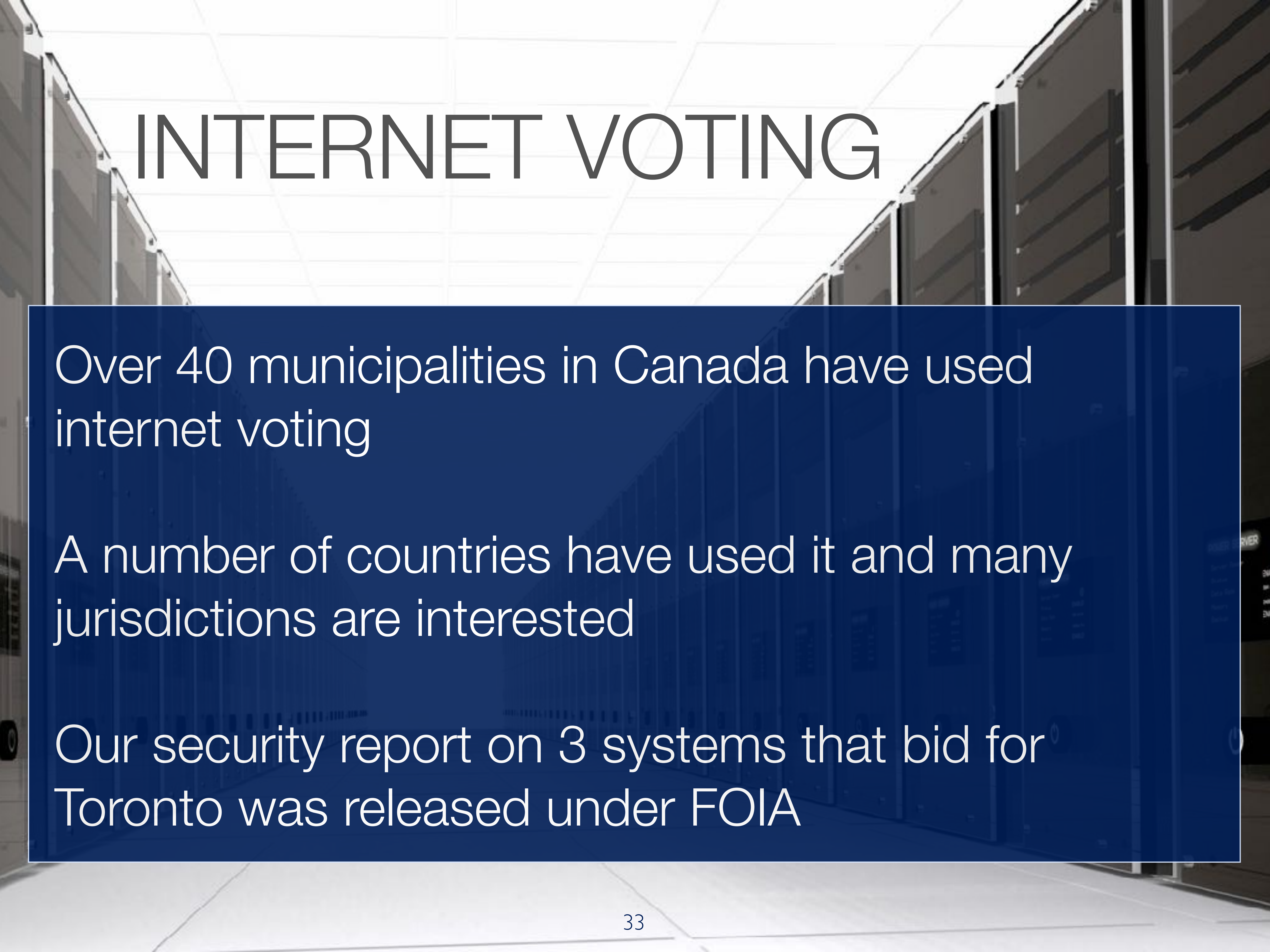
RESPONSE

Most voters found the process easy. The cryptography is opt-in and can essentially be ignored. Some voters liked the novelty of the system (turnout spiked after the local radio station covered the system)

Some voters did not realize they could verify elections, some complained about the pens, some found codes hard to read. Others disliked electronic voting in general or had difficulty with IRV

Poll workers found the election required more explanation and would like better voter education in future elections

Overall, response was generally positive

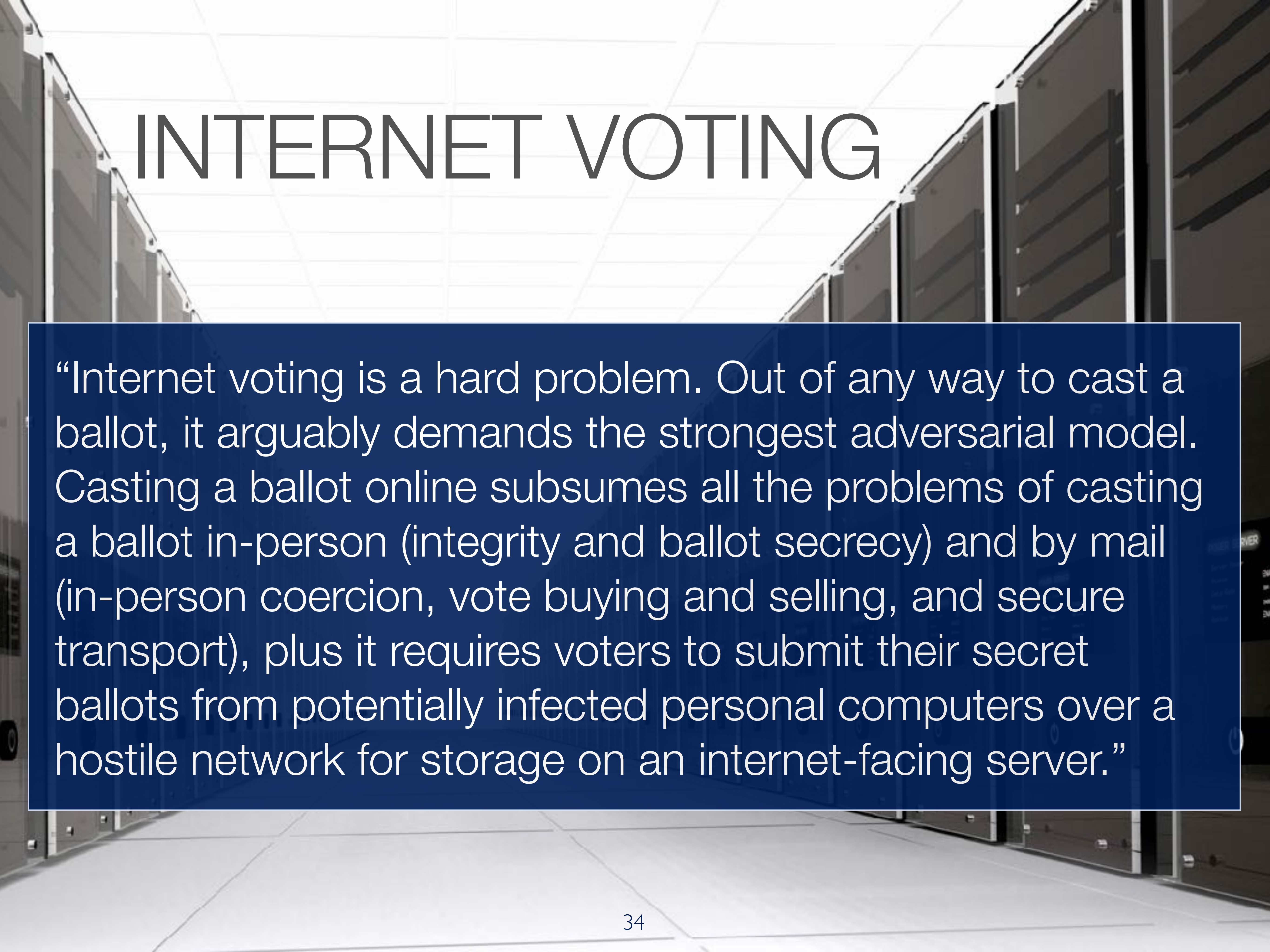


INTERNET VOTING

Over 40 municipalities in Canada have used internet voting

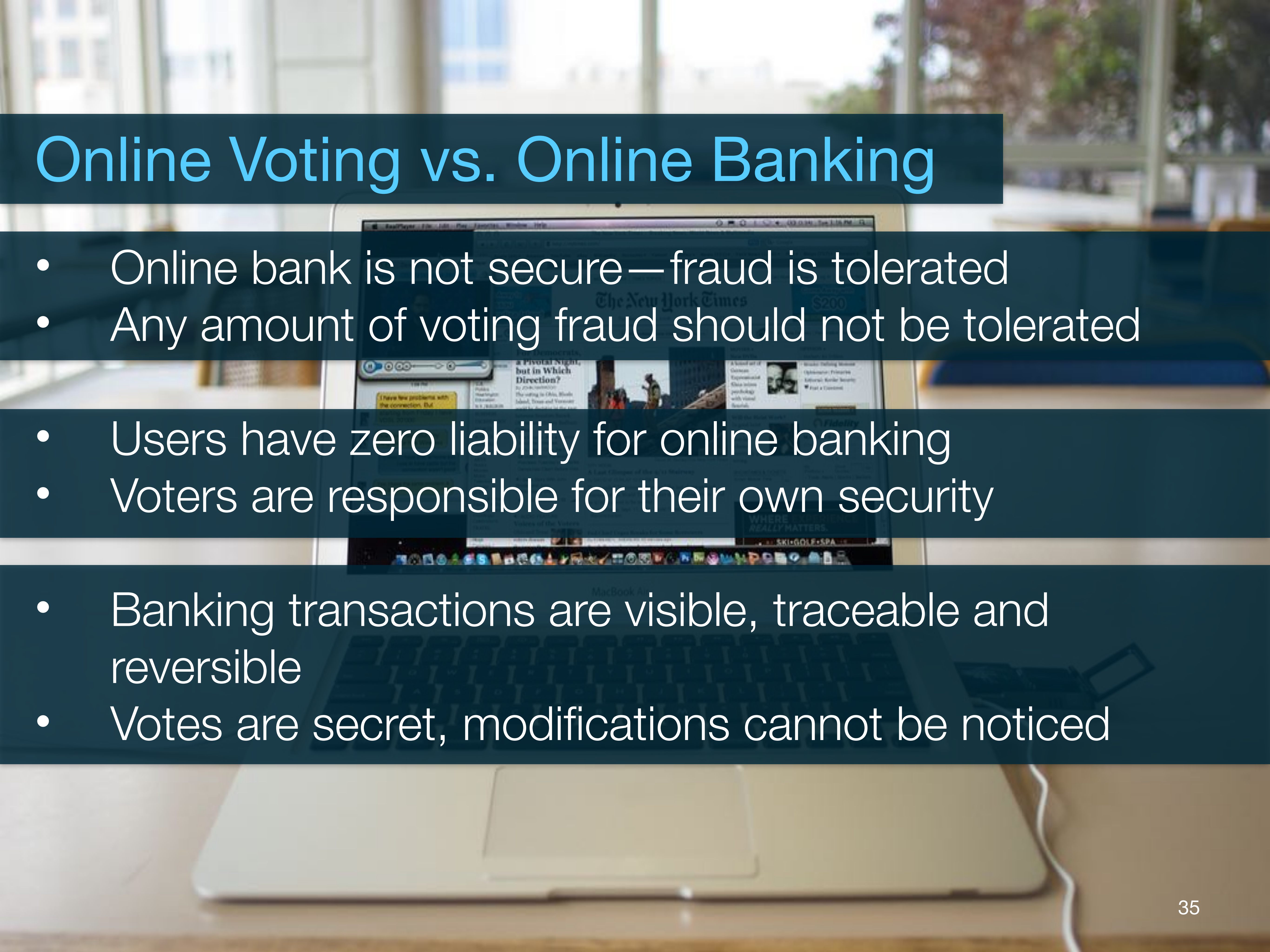
A number of countries have used it and many jurisdictions are interested

Our security report on 3 systems that bid for Toronto was released under FOIA



INTERNET VOTING

"Internet voting is a hard problem. Out of any way to cast a ballot, it arguably demands the strongest adversarial model. Casting a ballot online subsumes all the problems of casting a ballot in-person (integrity and ballot secrecy) and by mail (in-person coercion, vote buying and selling, and secure transport), plus it requires voters to submit their secret ballots from potentially infected personal computers over a hostile network for storage on an internet-facing server."



Online Voting vs. Online Banking

- Online bank is not secure—fraud is tolerated
- Any amount of voting fraud should not be tolerated

- Users have zero liability for online banking
- Voters are responsible for their own security

- Banking transactions are visible, traceable and reversible
- Votes are secret, modifications cannot be noticed

CURRENT WORK

Internet Voting: Instead of opposing, focus on building it as secure as possible. Project with City of Toronto under funding review. Home-visit program with hardened tablet and assistive technology

Delegative Democracy: Silicon Valley rediscovered and rebranded delegative democracy as “Liquid Democracy.” We are studying ballot secrecy in this space, as well as the social utility

Blockchains and Democracy: a new data structure from Bitcoin has been posited as useful for voting. We are generally critical but show limited and specific use cases

QUESTIONS?

Jeremy Clark

@PulpSpy

vaddr.space