

# STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System

Josh Benaloh (Microsoft Research)

Mike Byrne (Rice University)

Bryce Eakin (independent consultant)

Philip Kortum (Rice University)

Neal McBurnett (ElectionAudits)

Olivier Pereira (Université catholique de Louvain)

Philip B. Stark (University of California Berkeley)

**Dan S. Wallach** (Rice University)

*and the Travis County Elections Office Staff*



# A rare opportunity

**Dana DeBeauvoir (Travis County Clerk),  
Keynote speech, EVT/WOTE 2011**

***We're going to design a new voting system from  
scratch and we need your help.***

# Travis County (Austin, Texas)

**Population: ~1 million**

~392k votes cast November 2012

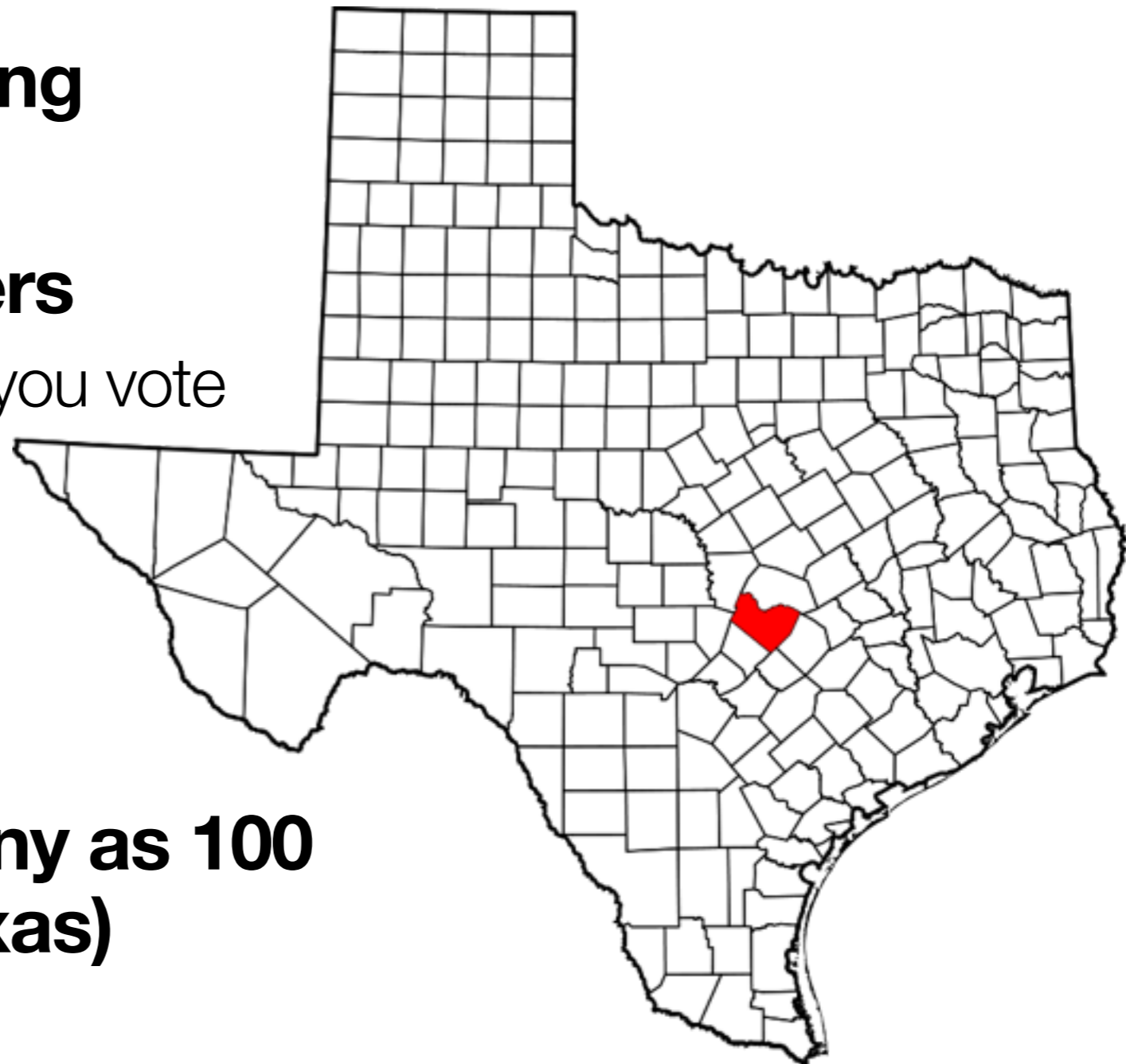
**Two weeks of early voting**

23 locations

**Election-day vote centers**

Every local precinct now lets you vote any ballot style in the county

**Ballots can have as many as 100 contests (typical for Texas)**



# Travis County voting technology

## Pre-2001: centrally tabulated optical scan ballots

Huge logistical challenges

## 2001: Hart InterCivic eSlate system

No ambiguity of voter intent

Good accessibility features

Fast results

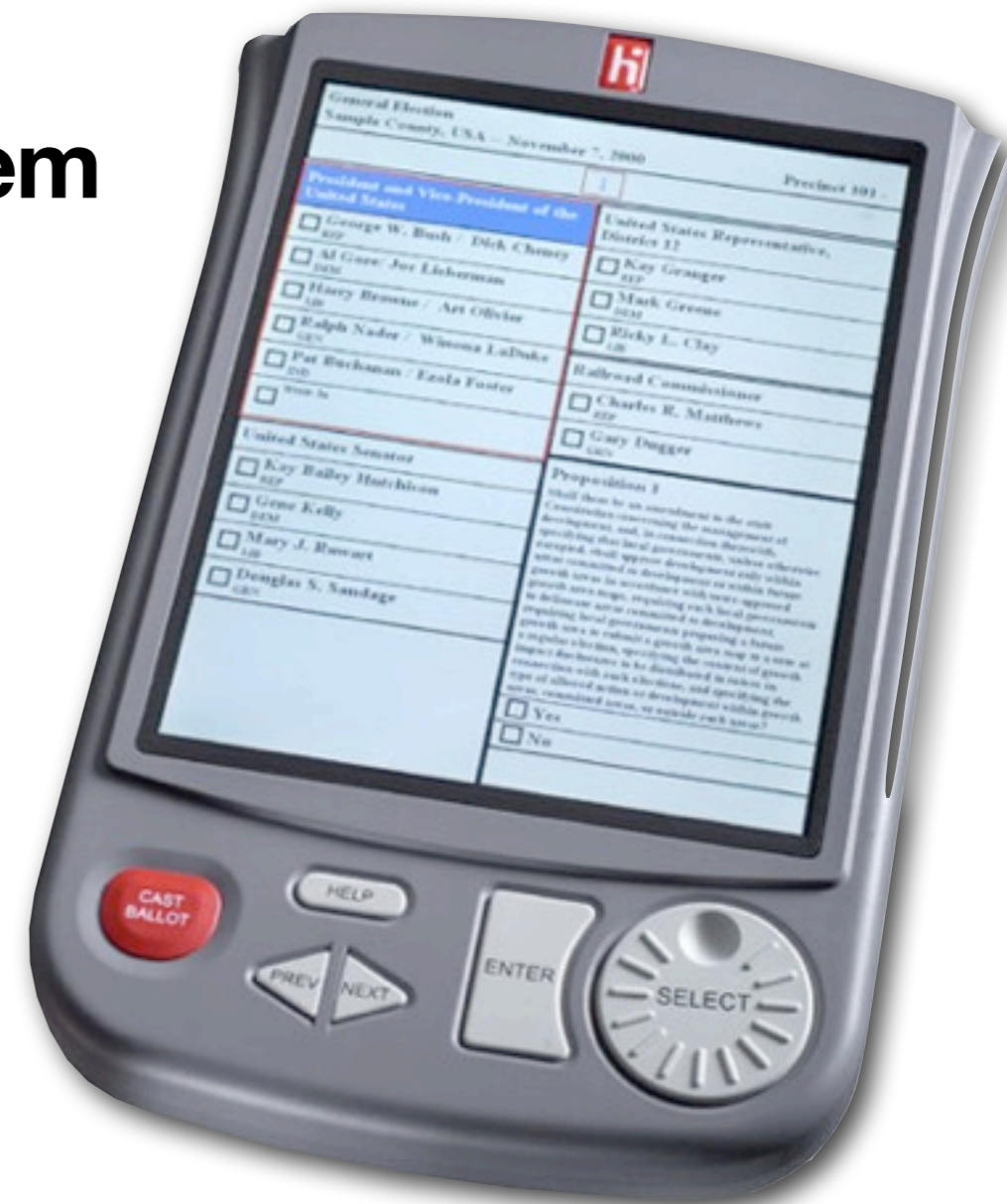
Unhappy activists

## 2011: Time for something new

eSlate systems reaching end of life

Nothing attractive on the market

**Crazy idea: call in the academics!**



# Constraint #1: DRE-style UI

## Consistent UI for all voters

Accessibility features (headphones, buttonbox, etc.)

Voter-intent disambiguated before they leave

## Off-the-shelf hardware

Commercial DRE equipment is

\$3000+ per machine

E.g., Sony Vaio Tap 20, ~\$1000

Cheaper support contracts as well

## Printer attached to the DRE

Machine-printed ballot goes into a ballot box



# Constraint #2: Paper ballots

## Tangible, hand-countable records of voter intent

*Machine-printed* to avoid ambiguous marks

Only show selected candidates, save lots of space

### Official Ballot November 4, 2012

Joint General and Special Elections  
Travis County, Texas Precinct 101A

11042012

Pct 101A

BID11042012

BCID3457894

Pg 1 of 2

Travis County General Election continued


#### Precinct 145, Justice of the Peace

PURP Nancy Nu 

#### District 147, State Representative

PURP Xena Xi 

#### County Judge

PURP Oscar Omicron 

#### County Court at Law 677, Judge

PURP Peggy Pi 

#### County Probate Court Judge

PURP Rhoda Rho 

#### District Clerk

PURP Samuel Sigma 

#### County Clerk

GLD Teresa Tau 

#### County Treasurer

PURP Uma Upsilon 

#### District Clerk

PURP Selena Sigma 

#### Travis County General Election

##### Straight Party

PURP Purple 

##### District 210, United States Representative

PURP Anna Alpha 

##### Governor

PURP Betty Beta 

##### Lieutenant Governor

PURP Gertrude Gamma 

##### Attorney General

PURP Daniel Delta 

##### State Senator

PURP Eric Epsilon 

##### Comptroller of Public Accounts

GLD Zitta Zeta 

##### Attorney General

PURP Derick Delta 

# Constraint #3: Vote centers

**Any voter can go to any precinct and vote**

Online voter registration database

*Offline* voting machines

Carefully limited data flows across the boundary

**Thousands of distinct ballot styles**

Pre-printed traditional ballots are untenable

# Constraint #4: All day battery

## **Power failures should not close the polls!**

12+ hours on battery is a requirement

## **Printers must be thermal**

Laser consumers too much power

Inkjet too unreliable

## **Touch screen computers with long-life batteries?**

Laptops vs. small tablets vs. big tablets

Sony Vaio Tap 20 can do 4 hours, idle with screen on dim

**Sophisticated new features**

# Sophisticated new features

## **VoteBox-style in-precinct network**

Local wired network (no Internet, no wireless)

Hash chaining, massive data replication

# Sophisticated new features

## **VoteBox-style in-precinct network**

Local wired network (no Internet, no wireless)

Hash chaining, massive data replication

## **E2E cryptography**

Homomorphic, verifiable tallies

Public bulletin board, full-election ciphertexts

# Sophisticated new features

## **VoteBox-style in-precinct network**

Local wired network (no Internet, no wireless)

Hash chaining, massive data replication

## **E2E cryptography**

Homomorphic, verifiable tallies

Public bulletin board, full-election ciphertexts

## **Evidence-based elections (risk limiting audits)**

Verify the paper corresponds to the electronic records

# Sophisticated new features

## **VoteBox-style in-precinct network**

Local wired network (no Internet, no wireless)

Hash chaining, massive data replication

## **E2E cryptography**

Homomorphic, verifiable tallies

Public bulletin board, full-election ciphertexts

## **Evidence-based elections (risk limiting audits)**

Verify the paper corresponds to the electronic records

## **Usability**

Help voters and poll workers

Ensure security features don't damage usability

# Workflow: Registration

Registration



# Workflow: Registration

Registration

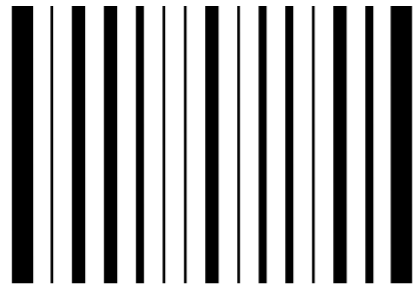


# Workflow: Registration

Registration



Precinct 101A



# Workflow: Authorization

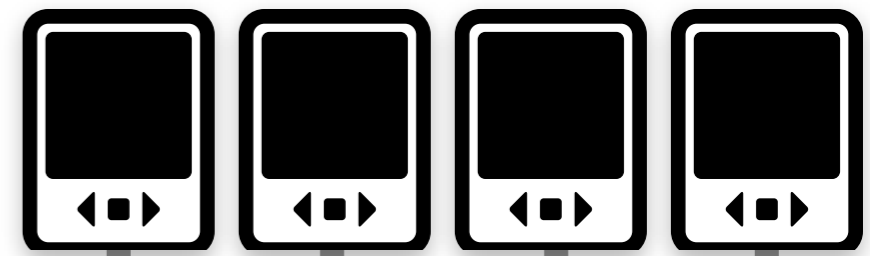
Registration



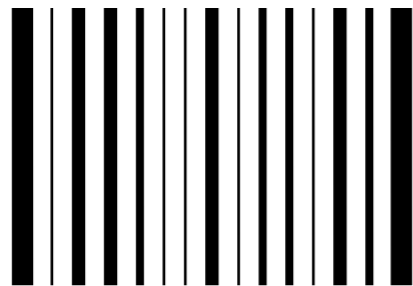
Controller



Voting terminals

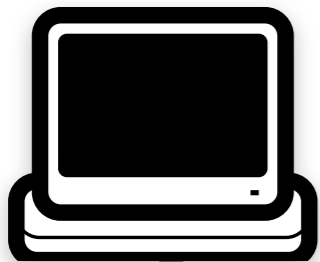


Precinct 101A

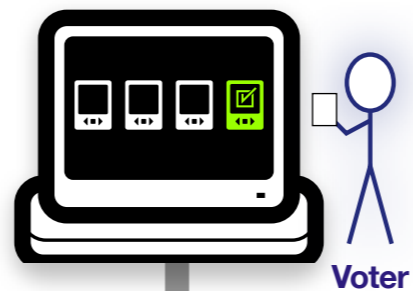


# Workflow: Authorization

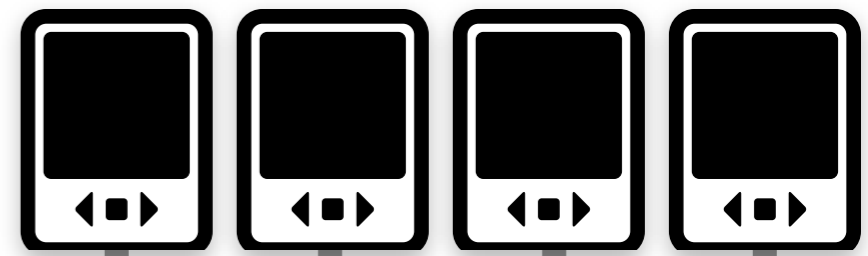
Registration



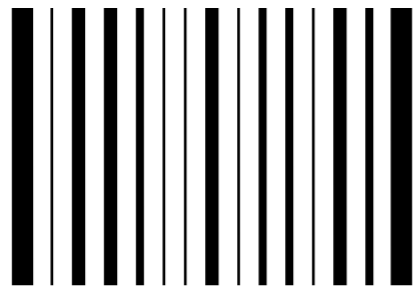
Controller



Voting terminals

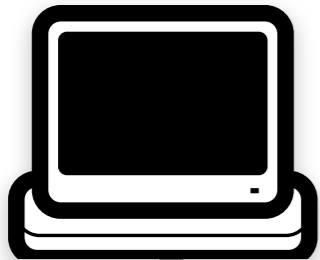


Precinct 101A

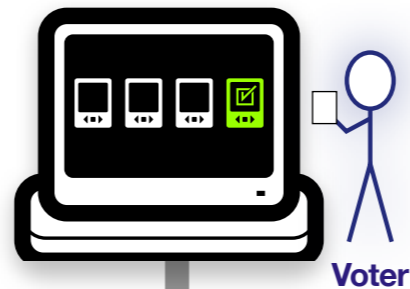


# Workflow: Authorization

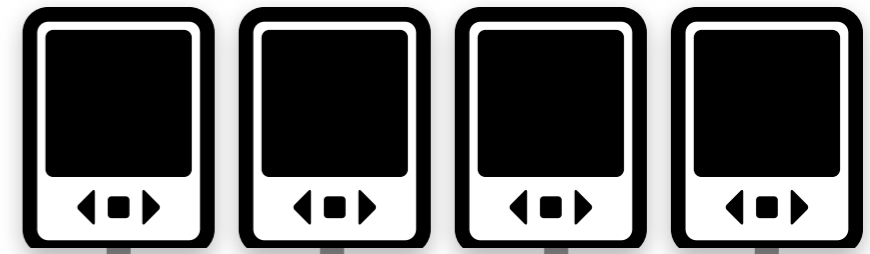
Registration



Controller



Voting terminals

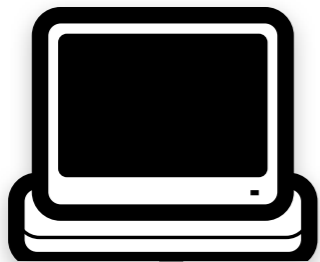


Auth: 52794

Similar to Hart InterCivic eSlate

# Workflow: Authorization

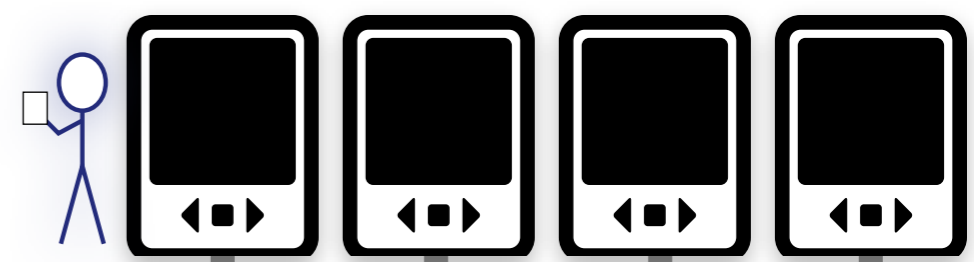
Registration



Controller



Voting terminals



Auth: 52794

Similar to Hart InterCivic eSlate

# Workflow: Voting

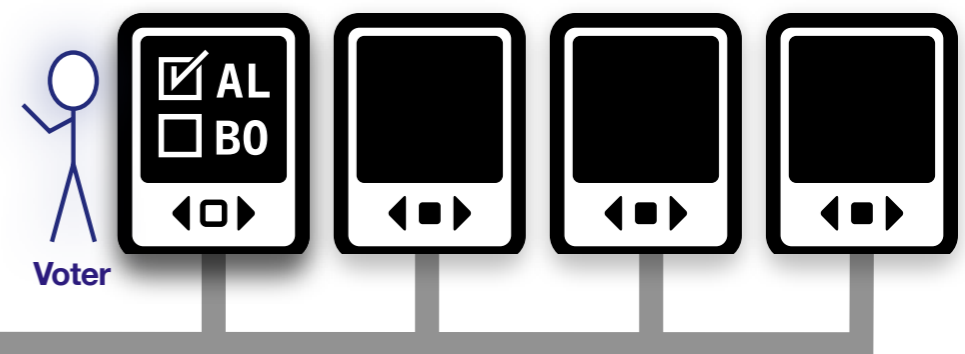
Registration



Controller

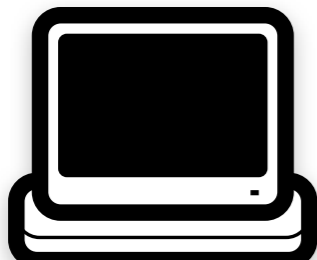


Voting terminals



# Workflow: Casting

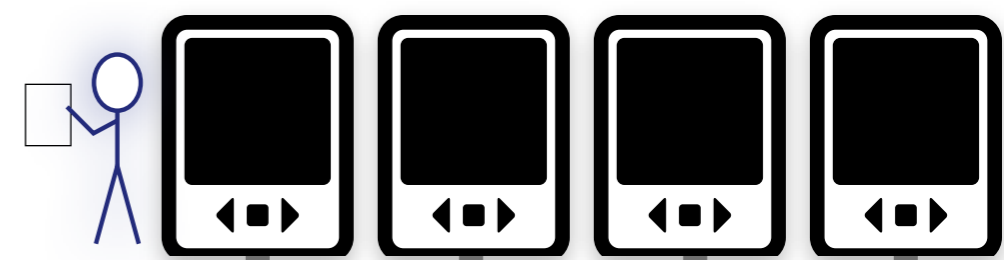
Registration



Controller



Voting terminals



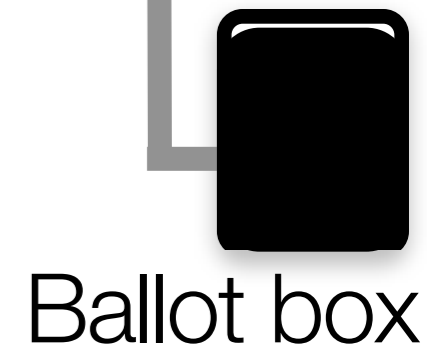
Voter

**Official Ballot November 4, 2012**  
 Joint General and Special Elections  
 Travis County, Texas Precinct 101A

11042012 Pct 101A B1011042012 BCID3457894 Pg 1 of 2

Travis County General Election continued  
 Precinct 145, Justice of the Peace

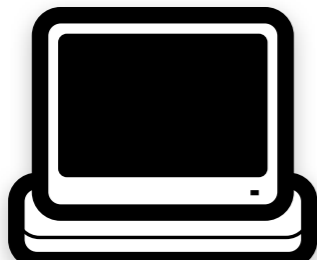
PURP	Nancy Nu	<input checked="" type="radio"/>
District 147, State Representative		
PURP	Xena Xi	<input checked="" type="radio"/>
County Judge		
PURP	Oscar Omicron	<input checked="" type="radio"/>
County Court at Law 677, Judge		
PURP	Peggy Pi	<input checked="" type="radio"/>
County Probate Court Judge		
PURP	Rhoda Rho	<input checked="" type="radio"/>
District Clerk		
PURP	Samuel Sigma	<input checked="" type="radio"/>
County Clerk		
GLD	Teresa Tau	<input checked="" type="radio"/>
County Treasurer		
PURP	Uma Upsilon	<input checked="" type="radio"/>
District Clerk		
PURP	Selena Sigma	<input checked="" type="radio"/>
County Clerk		
GLD	Thomas Tau	<input checked="" type="radio"/>
County Treasurer		
PURP	Ulysses Upsilon	<input checked="" type="radio"/>
County Commissioner		
PURP	Phillip Phi	<input checked="" type="radio"/>
Railroad Commissioner		
PURP	Charles Chi	<input checked="" type="radio"/>
Place 332, Justice, Supreme Court		
	NO SELECTION	<input type="radio"/>
Place 554, Justice, Supreme Court		
	NO SELECTION	<input type="radio"/>
Place 445, Justice, Supreme Court		
	NO SELECTION	<input type="radio"/>
Place 549, Justice, Supreme Court		
	NO SELECTION	<input type="radio"/>
Place 223, Judge, Court of Criminal Appeals		
	NO SELECTION	<input type="radio"/>
Place 552, Judge, Court of Criminal Appeals		
	NO SELECTION	<input type="radio"/>
Railroad Commissioner		
PURP	Isha Iota	<input checked="" type="radio"/>
Place 334, Justice, Supreme Court		
	NO SELECTION	<input type="radio"/>
Place 667, Judge, Court of Criminal Appeals		
	NO SELECTION	<input checked="" type="radio"/>
District 589, Member State Board of Education		
PURP	Kevin Kappa	<input checked="" type="radio"/>
District 257, State Senator		
	NO SELECTION	<input type="radio"/>



Ballot box

# Workflow: Casting

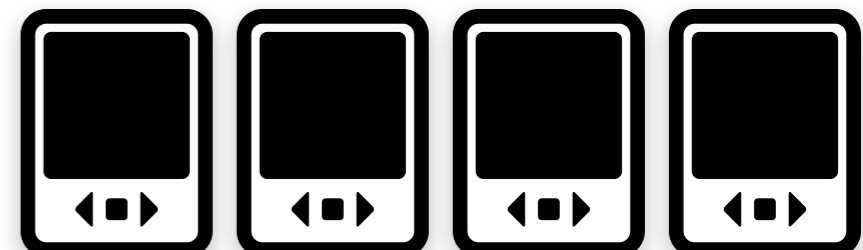
## Registration



## Controller



## Voting terminals



**Official Ballot November 4, 2012**  
Joint General and Special Elections  
Travis County, Texas Precinct 101A

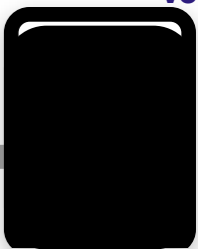
11042012 Pct 101A B111042012 BCID3457894 Pg 1 of 2

Travis County General Election continued  
Precinct 145, Justice of the Peace

<b>Travis County General Election</b>	
Straight Party	
PURP	Purple <input checked="" type="radio"/>
<b>District 210, United States Representative</b>	
PURP	Anna Alpha <input checked="" type="radio"/>
<b>Governor</b>	
PURP	Betty Beta <input checked="" type="radio"/>
<b>Lieutenant Governor</b>	
PURP	Gertrude Gamma <input checked="" type="radio"/>
<b>Attorney General</b>	
PURP	Daniel Delta <input checked="" type="radio"/>
<b>State Senator</b>	
PURP	Eric Epsilon <input checked="" type="radio"/>
<b>Comptroller of Public Accounts</b>	
GLD	Zitta Zeta <input checked="" type="radio"/>
<b>Attorney General</b>	
PURP	Derick Delta <input checked="" type="radio"/>
<b>State Senator</b>	
PURP	Edith Epsilon <input checked="" type="radio"/>
<b>Comptroller of Public Accounts</b>	
GLD	Zorro Zeta <input checked="" type="radio"/>
<b>Commissioner of the General Land Office</b>	
PURP	Etta Eta <input checked="" type="radio"/>
<b>Commissioner of Agriculture</b>	
PURP	Theodore Theta <input checked="" type="radio"/>
<b>Railroad Commissioner</b>	
PURP	Onne Iota <input checked="" type="radio"/>
<b>Place 334, Justice, Supreme Court</b>	
	NO SELECTION <input type="radio"/>
<b>Place 445, Justice, Supreme Court</b>	
	NO SELECTION <input type="radio"/>
<b>Place 549, Justice, Supreme Court</b>	
	NO SELECTION <input type="radio"/>
<b>Place 223, Judge, Court of Criminal Appeals</b>	
	NO SELECTION <input type="radio"/>
<b>Place 552, Judge, Court of Criminal Appeals</b>	
	NO SELECTION <input type="radio"/>
<b>Railroad Commissioner</b>	
PURP	Iesha Iota <input checked="" type="radio"/>
<b>Place 334, Justice, Supreme Court</b>	
	NO SELECTION <input type="radio"/>
<b>Place 667, Judge, Court of Criminal Appeals</b>	
	NO SELECTION <input type="radio"/>
<b>District 589, Member State Board of Education</b>	
PURP	Kevin Kappa <input checked="" type="radio"/>
<b>District 257, State Senator</b>	
	NO SELECTION <input type="radio"/>
<b>District 147, State Representative</b>	
PURP	Nancy Nu <input checked="" type="radio"/>
<b>County Judge</b>	
PURP	Xena Xi <input checked="" type="radio"/>
<b>County Court at Law 677, Judge</b>	
PURP	Oscar Omicron <input checked="" type="radio"/>
<b>County Probate Court Judge</b>	
PURP	Peggy Pi <input checked="" type="radio"/>
<b>District Clerk</b>	
PURP	Rhoda Rho <input checked="" type="radio"/>
<b>County Clerk</b>	
GLD	Samuel Sigma <input checked="" type="radio"/>
<b>County Treasurer</b>	
PURP	Teresa Tau <input checked="" type="radio"/>
<b>District Clerk</b>	
PURP	Uma Upsilon <input checked="" type="radio"/>
<b>County Clerk</b>	
GLD	Selena Sigma <input checked="" type="radio"/>
<b>County Treasurer</b>	
PURP	Thomas Tau <input checked="" type="radio"/>
<b>County Commissioner</b>	
PURP	Ulysses Upsilon <input checked="" type="radio"/>
<b>Railroad Commissioner</b>	
PURP	Phillip Phi <input checked="" type="radio"/>
<b>Place 332, Justice, Supreme Court</b>	
	Charles Chi <input checked="" type="radio"/>
<b>Place 554, Justice, Supreme Court</b>	
	NO SELECTION <input type="radio"/>
<b>Place 998, Justice, Supreme Court</b>	
	NO SELECTION <input type="radio"/>
<b>Place 221, Judge, Court of Criminal Appeals</b>	
	NO SELECTION <input type="radio"/>
<b>Place 155, Judge, Court of Criminal Appeals</b>	
	NO SELECTION <input type="radio"/>
<b>Place 166, Judge, Court of Criminal Appeals</b>	
	NO SELECTION <input type="radio"/>
<b>Place 332, Justice, Supreme Court</b>	
	NO SELECTION <input type="radio"/>
<b>Place 554, Justice, Supreme Court</b>	
	NO SELECTION <input type="radio"/>
<b>District 245, Member State Board of Education</b>	
PURP	Patrice Psi <input checked="" type="radio"/>
<b>Place 442, Justice, 33rd Court of Appeals District</b>	
PURP	Orlando Omega <input checked="" type="radio"/>



Voter



Ballot box

# Networked ballot box

**Notifies other machines that ballot was deposited**

Ballot has random ID

**Voter can spoil ballot and start over**

Usability win!

**Ballot box has no UI**

Deposit and done (just need a scanner for the ballot ID)

Cont



**Official Ballot November 4, 2012**  
Joint General and Special Elections  
Travis County, Texas Precinct 101A

11042012 Pct 101A BID11042012 BCI03457894 Pg 1 of 2

Travis County General Election continued

Travis County General Election	
Straight Party	PURP Purple
District 210, United States Representative	PURP Anna Alpha
Governor	PURP Betty Beta
Lieutenant Governor	PURP Gertrude Gamma
Attorney General	PURP Daniel Delta
State Senator	PURP Eric Epsilon
Comptroller of Public Accounts	GLD Zitta Zeta
Attorney General	PURP Derick Delta
State Senator	PURP Edith Epsilon
Comptroller of Public Accounts	GLD Zorro Zeta
Commissioner of the General Land Office	PURP Etta Eta
Commissioner of Agriculture	PURP Theodore Theta
Railroad Commissioner	PURP Onne Iota
Place 334, Justice, Supreme Court	NO SELECTION
Place 445, Justice, Supreme Court	NO SELECTION
Place 549, Justice, Supreme Court	NO SELECTION
Place 223, Judge, Court of Criminal Appeals	NO SELECTION
Place 552, Judge, Court of Criminal Appeals	NO SELECTION
Railroad Commissioner	PURP Iesha Iota
Place 334, Justice, Supreme Court	NO SELECTION
Place 667, Judge, Court of Criminal Appeals	NO SELECTION
District 589, Member State Board of Education	PURP Kevin Kappa
District 257, State Senator	NO SELECTION
Place 456, Justice, 33rd Court of Appeals District	PURP Larry Lambda
Place 334, Justice, Supreme Court	NO SELECTION
Place 667, Judge, Court of Criminal Appeals	NO SELECTION
District 589, Member State Board of Education	PURP Karla Kappa
District 257, State Senator	NO SELECTION
Place 456, Justice, 33rd Court of Appeals District	PURP Leticia Lambda

Precinct 145, Justice of the Peace	PURP Nancy Nu
District 147, State Representative	PURP Xena Xi
County Judge	PURP Oscar Omicron
County Court at Law 677, Judge	PURP Peggy Pi
County Probate Court Judge	PURP Rhoda Rho
District Clerk	PURP Samuel Sigma
County Clerk	GLD Teresa Tau
County Treasurer	PURP Uma Upsilon
District Clerk	PURP Selena Sigma
County Clerk	GLD Thomas Tau
County Treasurer	PURP Ulysses Upsilon
County Commissioner	PURP Phillip Phi
Railroad Commissioner	PURP Charles Chi
Place 332, Justice, Supreme Court	NO SELECTION
Place 554, Justice, Supreme Court	NO SELECTION
Place 998, Justice, Supreme Court	NO SELECTION
Place 221, Judge, Court of Criminal Appeals	NO SELECTION
Place 155, Judge, Court of Criminal Appeals	NO SELECTION
Place 166, Judge, Court of Criminal Appeals	NO SELECTION
Place 332, Justice, Supreme Court	NO SELECTION
Place 554, Justice, Supreme Court	NO SELECTION
District 245, Member State Board of Education	PURP Patrice Psi
Place 442, Justice, 33rd Court of Appeals District	PURP Orlando Omega

**Central Health Tax Ratification Election**

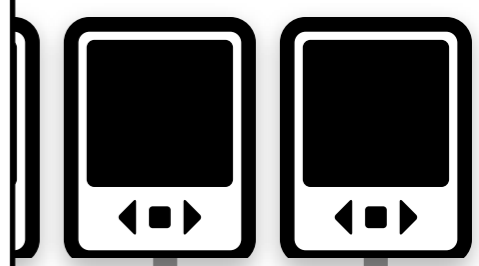
Propositon 1	For
Propositon 2	Against
Propositon 3	For

**Austin Community College Board of Trustees Election**

Place 7, ACC Trustee	Umberto Upsilon
----------------------	-----------------

11042012 Pct 101A BID11042012 BCI03457894 Pg 1 of 2

iminals



Ballot box

# Networked ballot box

**Notifies other machines that ballot was deposited**

Ballot has random ID

**Voter can spoil ballot and start over**

Usability win!

**Ballot box has no UI**

Deposit and done (just need a scanner for the ballot ID)

**Official Ballot November 4, 2012**  
Joint General and Special Elections  
Travis County, Texas Precinct 101A

11042012 Pct 101A BID11042012 BCI03457894 Pg 1 of 2

Travis County General Election continued

<b>Travis County General Election</b>	
Straight Party	PURP Purple <input checked="" type="radio"/>
District 210, United States Representative	PURP Anna Alpha <input checked="" type="radio"/>
Governor	PURP Betty Beta <input checked="" type="radio"/>
Lieutenant Governor	PURP Gertrude Gamma <input checked="" type="radio"/>
Attorney General	PURP Daniel Delta <input checked="" type="radio"/>
State Senator	PURP Eric Epsilon <input checked="" type="radio"/>
Comptroller of Public Accounts	GLD Zitta Zeta <input checked="" type="radio"/>
Attorney General	PURP Derick Delta <input checked="" type="radio"/>
State Senator	PURP Edith Epsilon <input checked="" type="radio"/>
Comptroller of Public Accounts	GLD Zorro Zeta <input checked="" type="radio"/>
Commissioner of the General Land Office	PURP Etta Eta <input checked="" type="radio"/>
Commissioner of Agriculture	PURP Theodore Theta <input checked="" type="radio"/>
Railroad Commissioner	PURP Onne Iota <input checked="" type="radio"/>
Place 334, Justice, Supreme Court	NO SELECTION <input type="radio"/>
Place 445, Justice, Supreme Court	NO SELECTION <input type="radio"/>
Place 549, Justice, Supreme Court	NO SELECTION <input type="radio"/>
Place 223, Judge, Court of Criminal Appeals	NO SELECTION <input type="radio"/>
Place 552, Judge, Court of Criminal Appeals	NO SELECTION <input type="radio"/>
Railroad Commissioner	PURP Iesha Iota <input checked="" type="radio"/>
Place 334, Justice, Supreme Court	NO SELECTION <input type="radio"/>
Place 667, Judge, Court of Criminal Appeals	NO SELECTION <input type="radio"/>
District 589, Member State Board of Education	PURP Kevin Kappa <input checked="" type="radio"/>
District 257, State Senator	NO SELECTION <input type="radio"/>
Place 456, Justice, 33rd Court of Appeals District	PURP Larry Lambda <input checked="" type="radio"/>
Place 334, Justice, Supreme Court	NO SELECTION <input type="radio"/>
Place 667, Judge, Court of Criminal Appeals	NO SELECTION <input type="radio"/>
District 589, Member State Board of Education	PURP Karla Kappa <input checked="" type="radio"/>
District 257, State Senator	NO SELECTION <input type="radio"/>
Place 456, Justice, 33rd Court of Appeals District	PURP Leticia Lambda <input checked="" type="radio"/>

<b>Precinct 145, Justice of the Peace</b>	PURP Nancy Nu <input checked="" type="radio"/>
District 147, State Representative	PURP Xena Xi <input checked="" type="radio"/>
County Judge	PURP Oscar Omicron <input checked="" type="radio"/>
County Court at Law 677, Judge	PURP Peggy Pi <input checked="" type="radio"/>
County Probate Court Judge	PURP Rhoda Rho <input checked="" type="radio"/>
District Clerk	PURP Samuel Sigma <input checked="" type="radio"/>
County Clerk	GLD Teresa Tau <input checked="" type="radio"/>
County Treasurer	PURP Uma Upsilon <input checked="" type="radio"/>
District Clerk	PURP Selena Sigma <input checked="" type="radio"/>
County Clerk	GLD Thomas Tau <input checked="" type="radio"/>
County Treasurer	PURP Ulysses Upsilon <input checked="" type="radio"/>
County Commissioner	PURP Phillip Phi <input checked="" type="radio"/>
Railroad Commissioner	PURP Charles Chi <input checked="" type="radio"/>
Place 332, Justice, Supreme Court	NO SELECTION <input type="radio"/>
Place 554, Justice, Supreme Court	NO SELECTION <input type="radio"/>
Place 998, Justice, Supreme Court	NO SELECTION <input type="radio"/>
Place 221, Judge, Court of Criminal Appeals	NO SELECTION <input type="radio"/>
Place 155, Judge, Court of Criminal Appeals	NO SELECTION <input type="radio"/>
Place 166, Judge, Court of Criminal Appeals	NO SELECTION <input type="radio"/>
Place 332, Justice, Supreme Court	NO SELECTION <input type="radio"/>
Place 554, Justice, Supreme Court	NO SELECTION <input type="radio"/>
District 245, Member State Board of Education	PURP Patrice Psi <input checked="" type="radio"/>
Place 442, Justice, 33rd Court of Appeals District	PURP Orlando Omega <input checked="" type="radio"/>

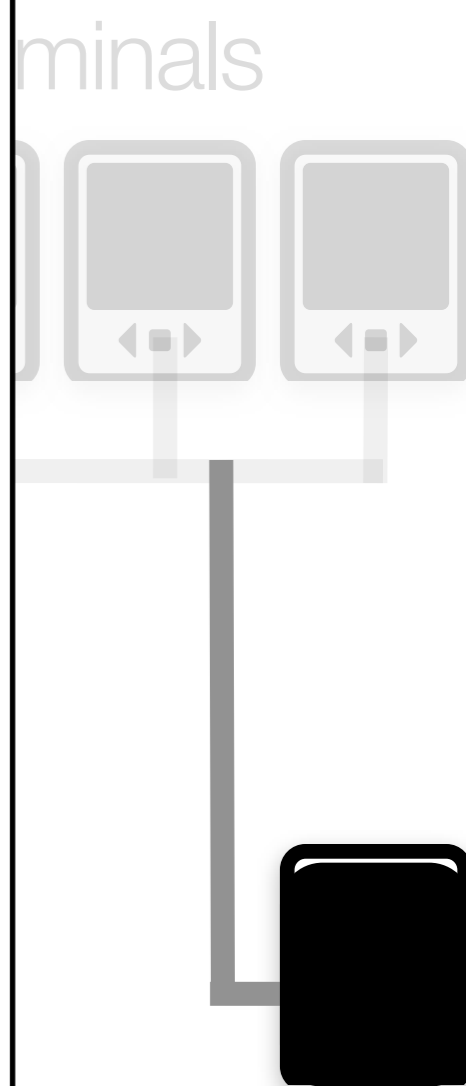
**Central Health Tax Ratification Election**

Propositon 1	For <input checked="" type="radio"/>
Propositon 2	Against <input checked="" type="radio"/>
Propositon 3	For <input checked="" type="radio"/>

**Austin Community College Board of Trustees Election**

Place 7, ACC Trustee	Umberto Upsilon <input checked="" type="radio"/>
----------------------	--

11042012 Pct 101A BID11042012 BCI03457894 Pg 1 of 2



Ballot box

# Catch the machine if it cheats!

**Benaloh challenges [2006]**

# Catch the machine if it cheats!

**Benaloh challenges [2006]**

**voter makes  
selections**

# Catch the machine if it cheats!

## Benaloh challenges [2006]

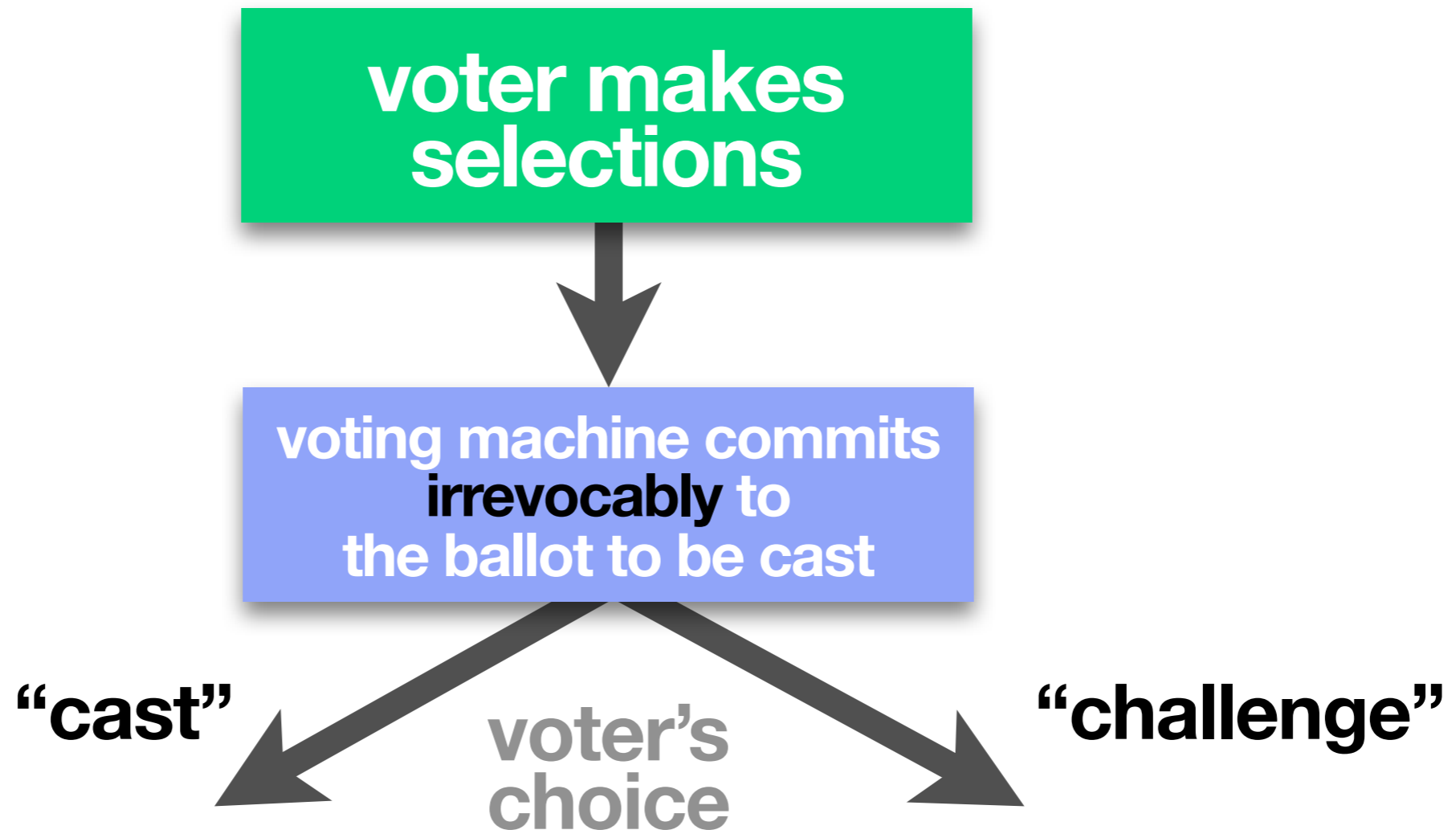
voter makes  
selections

```
graph TD; A[voter makes selections] --> B[voting machine commits irrevocably to the ballot to be cast];
```

voting machine commits  
**irrevocably** to  
the ballot to be cast

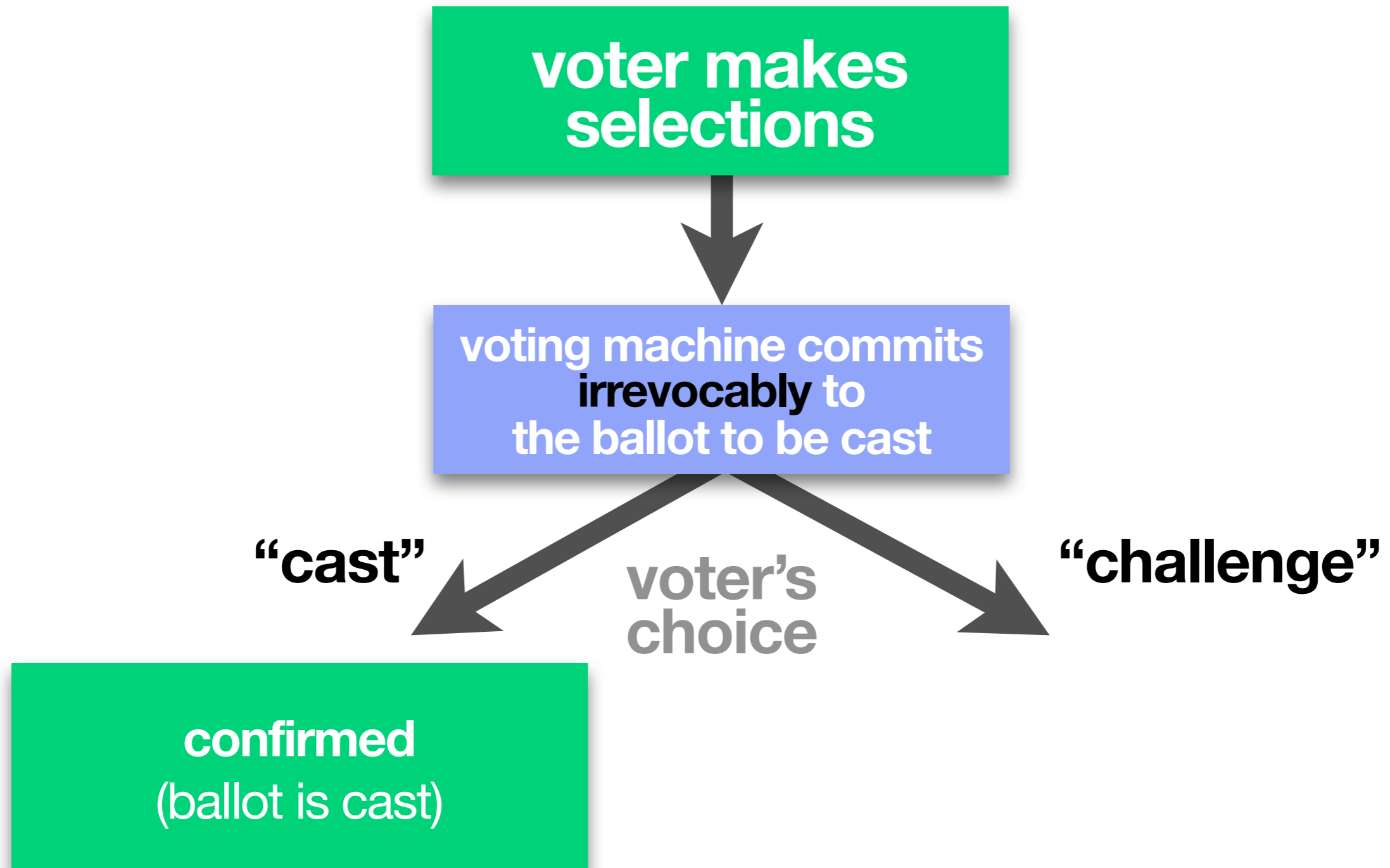
# Catch the machine if it cheats!

## Benaloh challenges [2006]



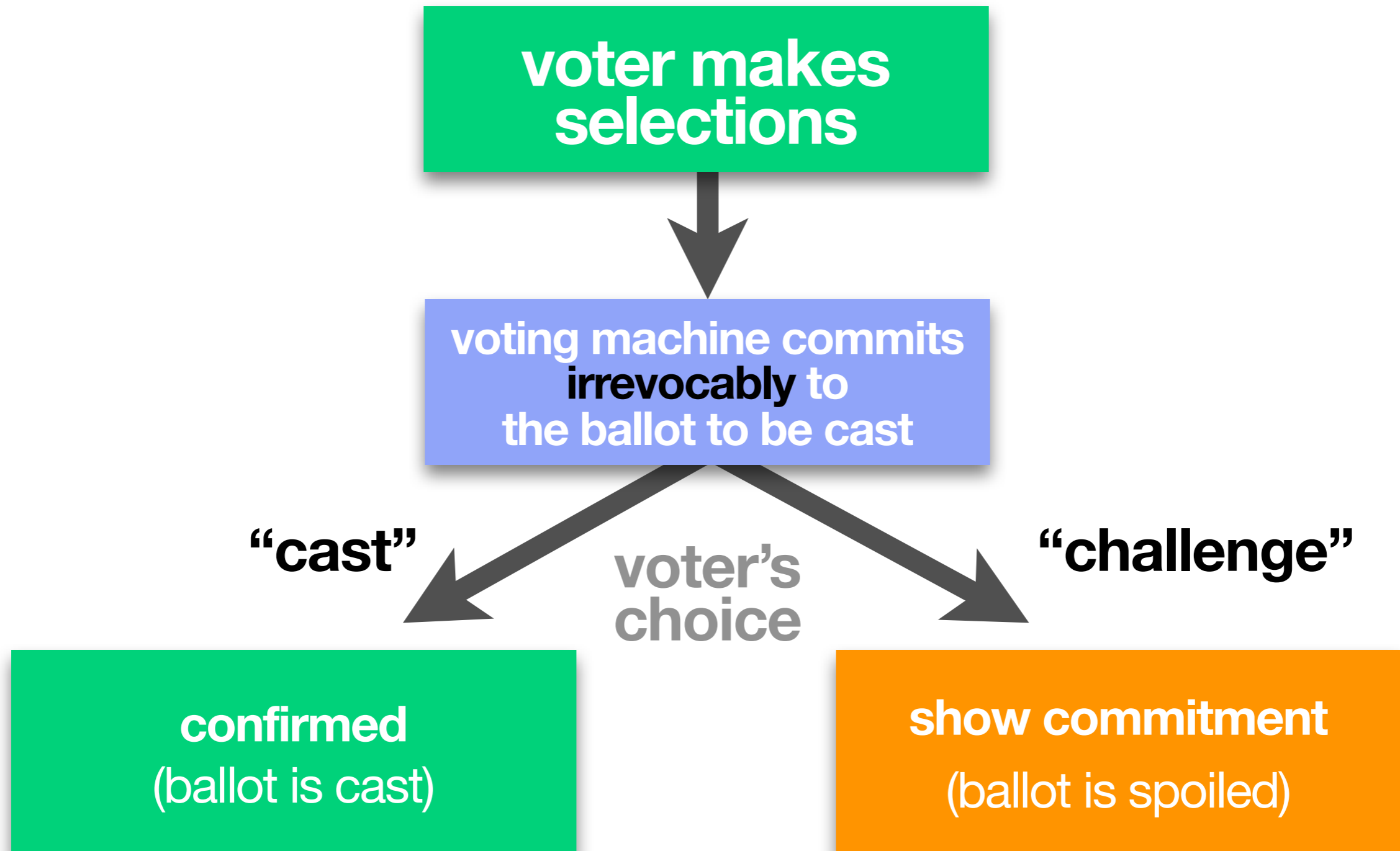
# Catch the machine if it cheats!

## Benaloh challenges [2006]



# Catch the machine if it cheats!

## Benaloh challenges [2006]



# Benaloh challenges in practice

**Original idea: print ciphertext behind opaque plate**

**Helios: hash sent to voter**

**VoteBox: ciphertext published on LAN**

**All require asking the voter to *cast* or *challenge***

*Significant usability problem*

# STAR challenges

## **Commitment: ciphertext broadcast to terminals**

Happens when the ballot is printed, just like VoteBox

## **Challenge: voter deposits or keeps ballot**

Challenger takes home printed ballot

Ballots that aren't deposited are decrypted, posted

*Procedurally: same as a spoiled ballot*

## **Big usability win**

*No need to ask the voter a challenge question*

Simple “live parallel testing”

# Post-election verification

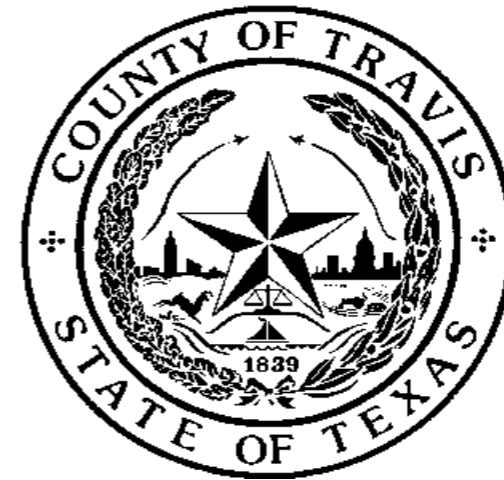
## Separate page to take home

Ballot hash for lookup on public bulletin board

***Cast ballot:***  
**ciphertext will match**

***Challenge ballot:***  
**plaintext also present, verifiable**

## YOUR VOTE COUNTS



**Thank you for voting!**

Take this confirmation of voting with you

Verify your ballot at:

[www.star-vote.org/ballot/HV1235Z7568RK84](http://www.star-vote.org/ballot/HV1235Z7568RK84)

Or, scan this code with your phone:



Find your code on the STAR-Vote website to ensure that your vote was recorded correctly.

Look for Election results and other tools for confirming the election at:  
[www.traviscountyelections.org](http://www.traviscountyelections.org)

Voting Date: October 30, 2012

Location: Randall's South Mopac

Voting Terminal: UI12345

Time: 18:45:56

**But what if  
something  
goes wrong?**

# Risk limiting audits (SOBA)

## **Random sampling of individual paper ballots**

Each should exactly match up with electronic records

Successful in a number of op-scan elections in California

## **STAR + SOBA: Requires decrypting ballots**

Post-election audit process

Only decrypt ballots as needed for the audit

*Requires touching tens of ballots, maybe hundreds, unlikely more*

# **Threat Mitigation**

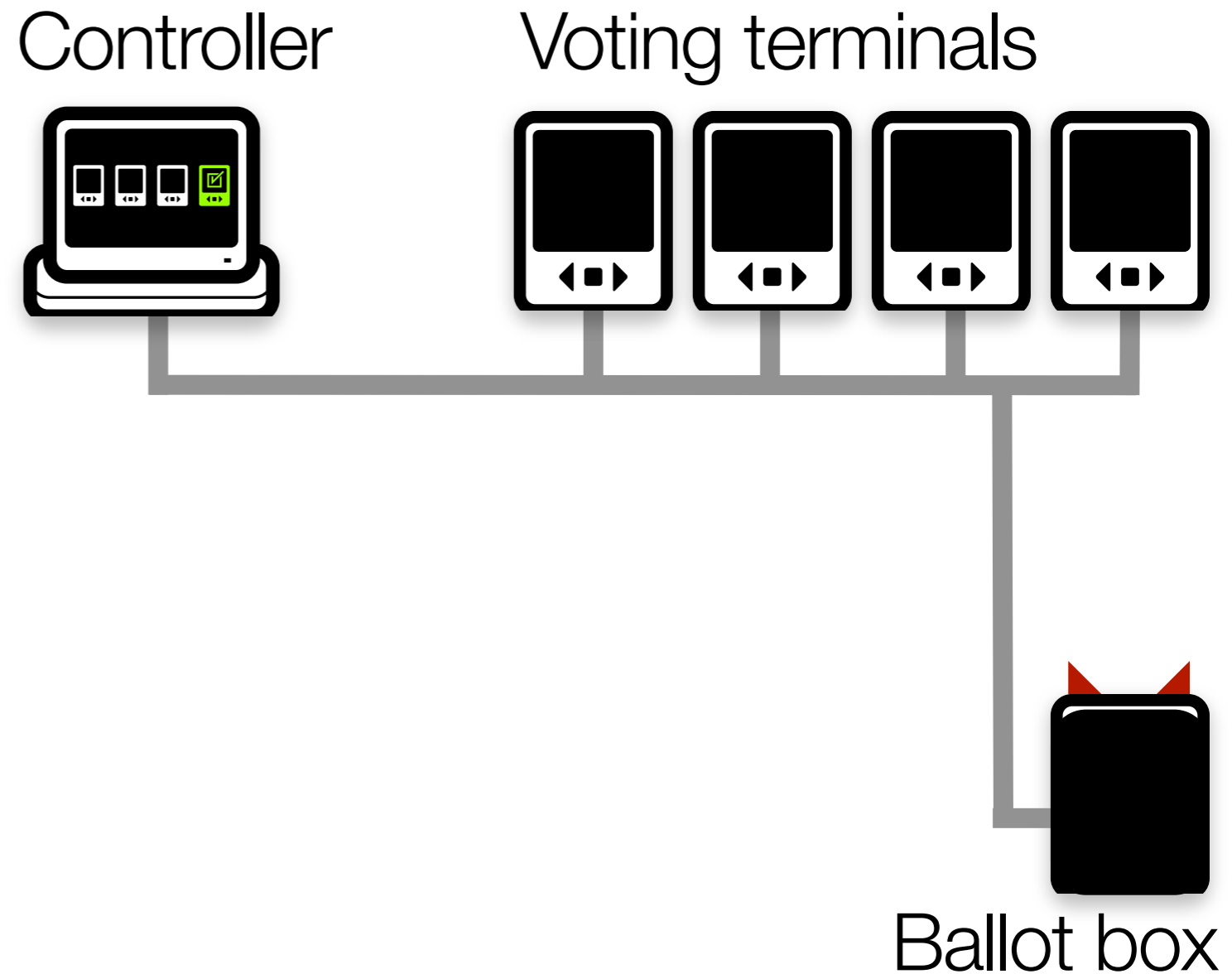
# Paper ballot stuffing?

## Primary tallies use electronic ballots

Paper without corresponding ciphertext is suspicious

## Chain voting

Detect/reject based on timestamps



# Malicious machine? (privacy)

**Record plaintext ballots in order cast**

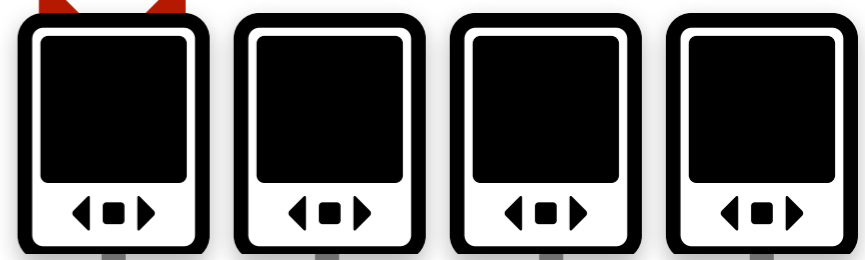
*(or subliminal channels)*

Fundamental problem!

Controller



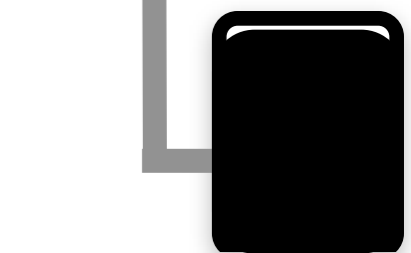
Voting terminals



**Work-in-progress solution: *trusted platform management (TPM)***

Terminals refuse to boot unsigned code

Integrity attestations broadcast to network



Ballot box

# Status

## **VoteBox-based proof-of-concept in progress**

Production system would want to start from scratch

## **Design mostly set**

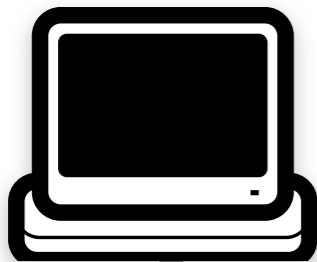
## **RFP almost ready to launch**

## **Publication**

Bell et al., *USENIX Journal of Election Technology & Systems (JETTS)*, vol 1., no. 1, August 2013.

# STAR-Vote: It's happening

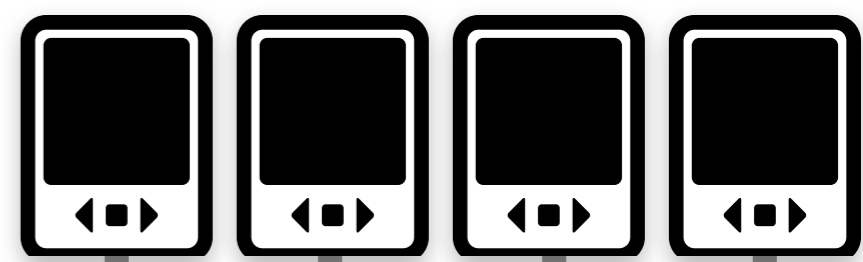
Registration



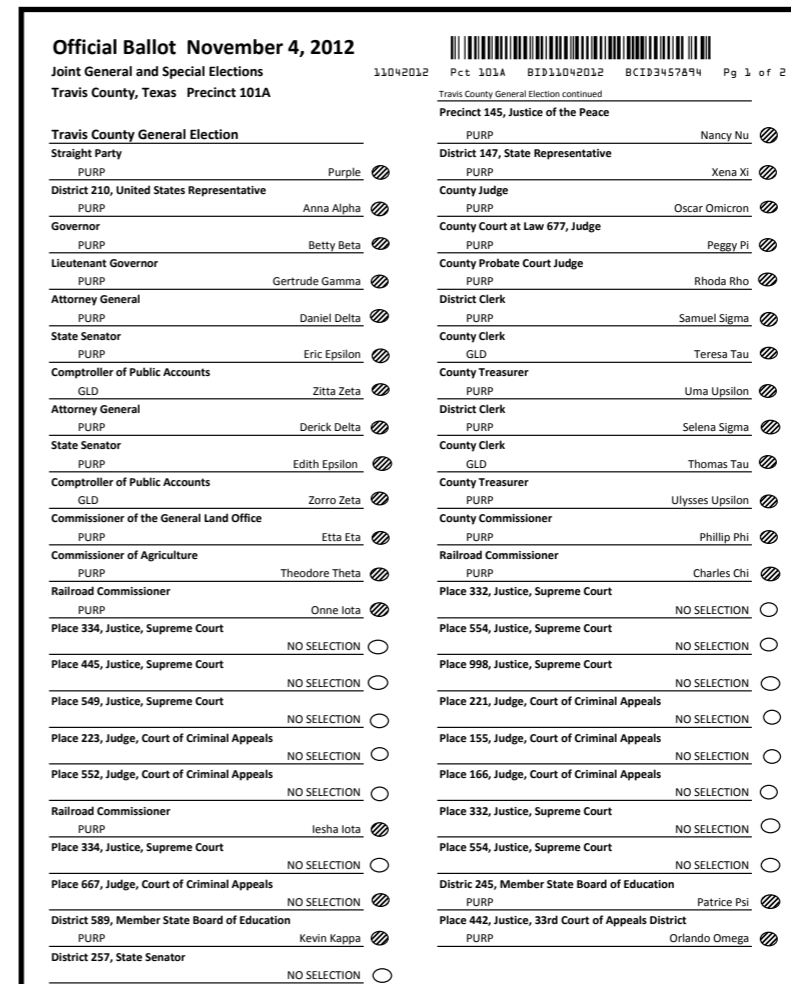
Controller



Voting terminals



**E2E verification**  
**Risk-limiting audits**  
**Tons of redundancy**  
**Usability/accessibility**  
**COTS hardware**



Ballot box

# Acknowledgements

## **ACCURATE** - A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections

Premiere NSF research center on e-voting, 2005-2011

Many ideas in STAR were developed in ACCURATE



## **NSF SaTC Medium: Voting Systems Architectures for Security and Usability**

Research support for STAR effort, 2014-2018

## **Microsoft SEIF**

Investigating integration of Win8 measured boot (2013+)

