
COMPUTER SECURITY LAB
RICE UNIVERSITY

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!

First meeting: April 2012

Long weekend in Austin

Olivier flew in on his own money

Josh took vacation time from Microsoft

Travis County elections staff + 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

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

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

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

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

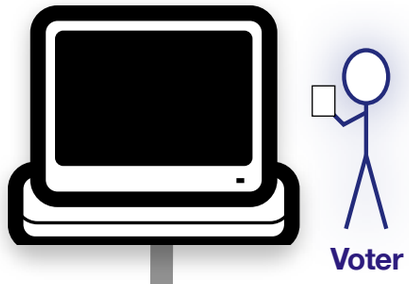
Registration



Precinct 101A

Workflow: Authorization

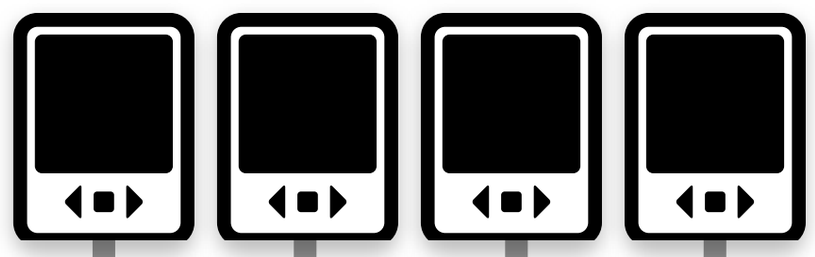
Registration

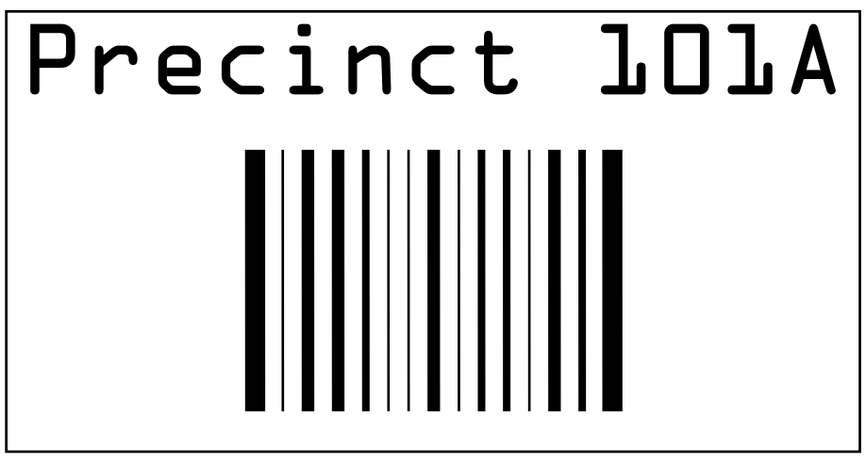


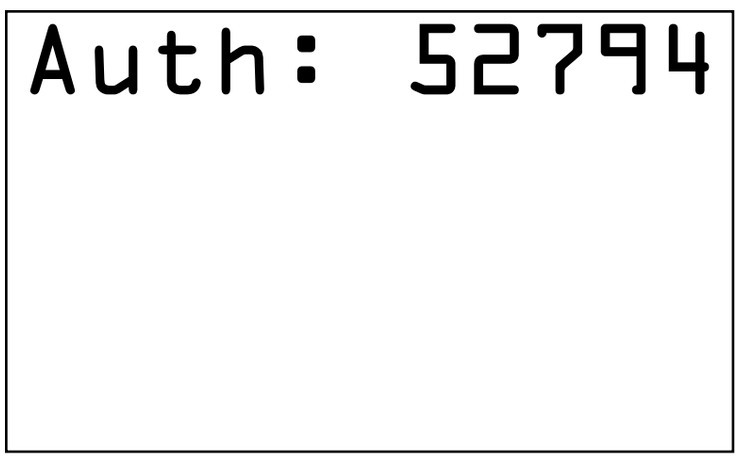
Controller



Voting terminals

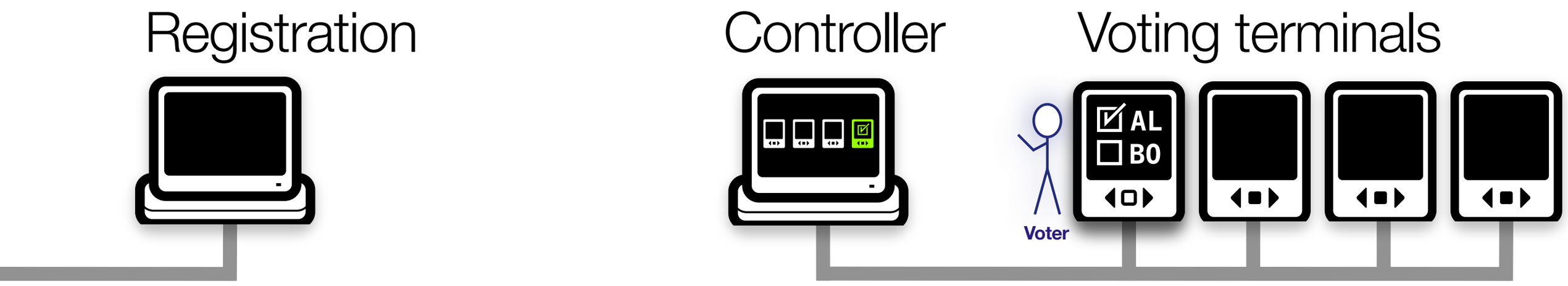




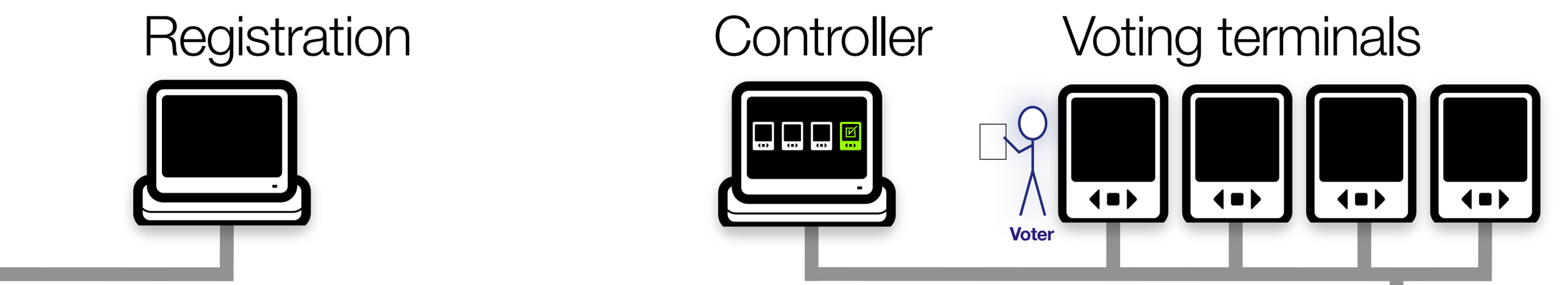


Similar to Hart InterCivic eSlate

Workflow: Voting



Workflow: Casting



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

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

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

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

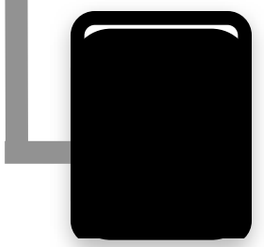
Place 166, Judge, Court of Criminal Appeals
NO SELECTION

Place 332, Justice, Supreme Court
NO SELECTION

Place 554, Justice, Supreme Court
NO SELECTION

Distric 245, Member State Board of Education
PURP — Patrice Psi

Place 442, Justice, 33rd Court of Appeals District
PURP — Orlando Omega



Ballot box

Networked ballot box

Notifies other machines that ballot was deposited

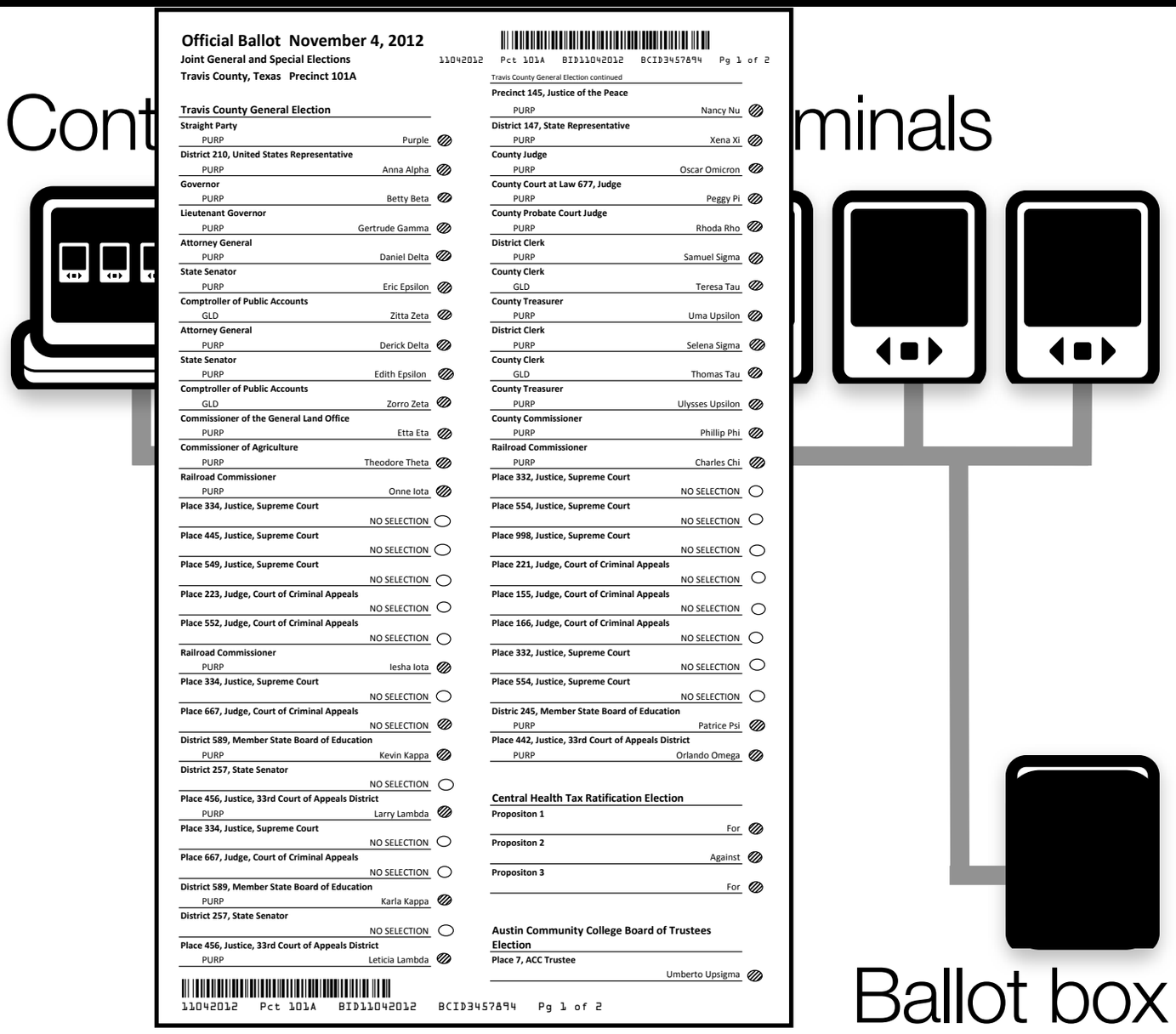
Ballot has random ID

Voter can spoil ballot and start over

Usability win!

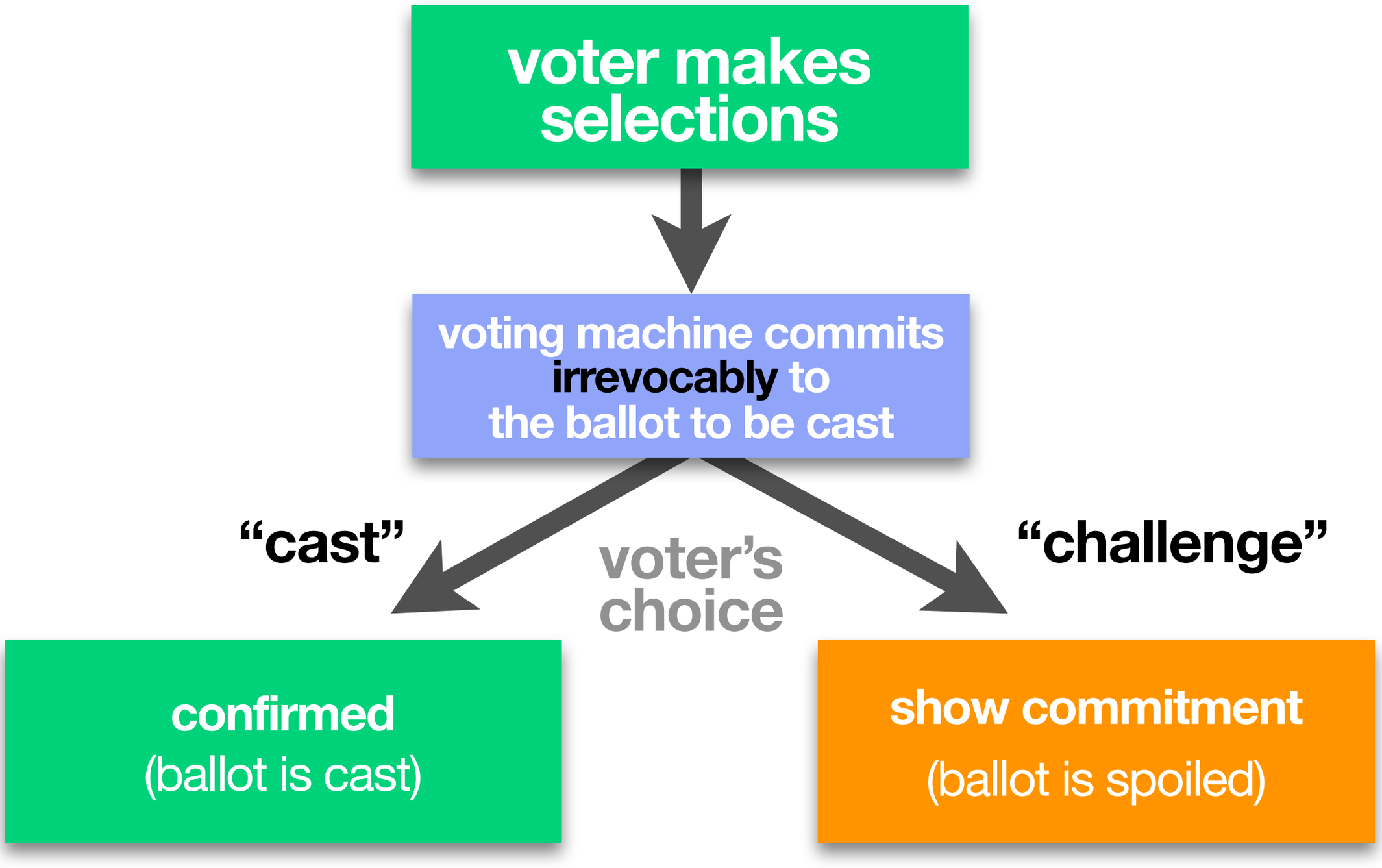
Ballot box has no UI

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



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

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

Voting Date: October 30, 2012
Voting Terminal: UI12345

Location: Randall's South Mopac
Time: 18:45:56

Cryptography outline

Every machine: public key for signing messages

Election authority is a CA

Every message: signed, broadcast, logged

Plus a hash of the sender's log head

Tamper-evident, resilient history of what happened

Every ballot: exponential Elgamal counters

Encrypted with public key of election authority

Homomorphic tallying, standard kludge for write-ins

Every counter includes "zero or one" NIZK proof

Threshold crypto for decryption key

Trustees decrypt election totals, challenge ballots

E2E properties verifiable

***Challenge ballots*: match up to plaintext receipt**

***Any ballot*: appears on the bulletin board**

***Homomorphic tallying*: provably includes all ballots on the bulletin board**

***Hash chains*: also publicly verifiable**

E2E verification process

***Easy*: voter visits URL, server does computation**

***Better*: voter runs open-source tool (provided)**

```
if (voter == “Josh Benaloh”)
    do_not_cheat = True
```

***Alternative*: voter gives receipt to political party, civic organization, newspaper, etc.**

Each organization’s smartphone app could scan the QRcode

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

Version 1: reencryption mixnet to an auditor key

Version 2: work in progress, no need for mixnet

Threat Mitigation

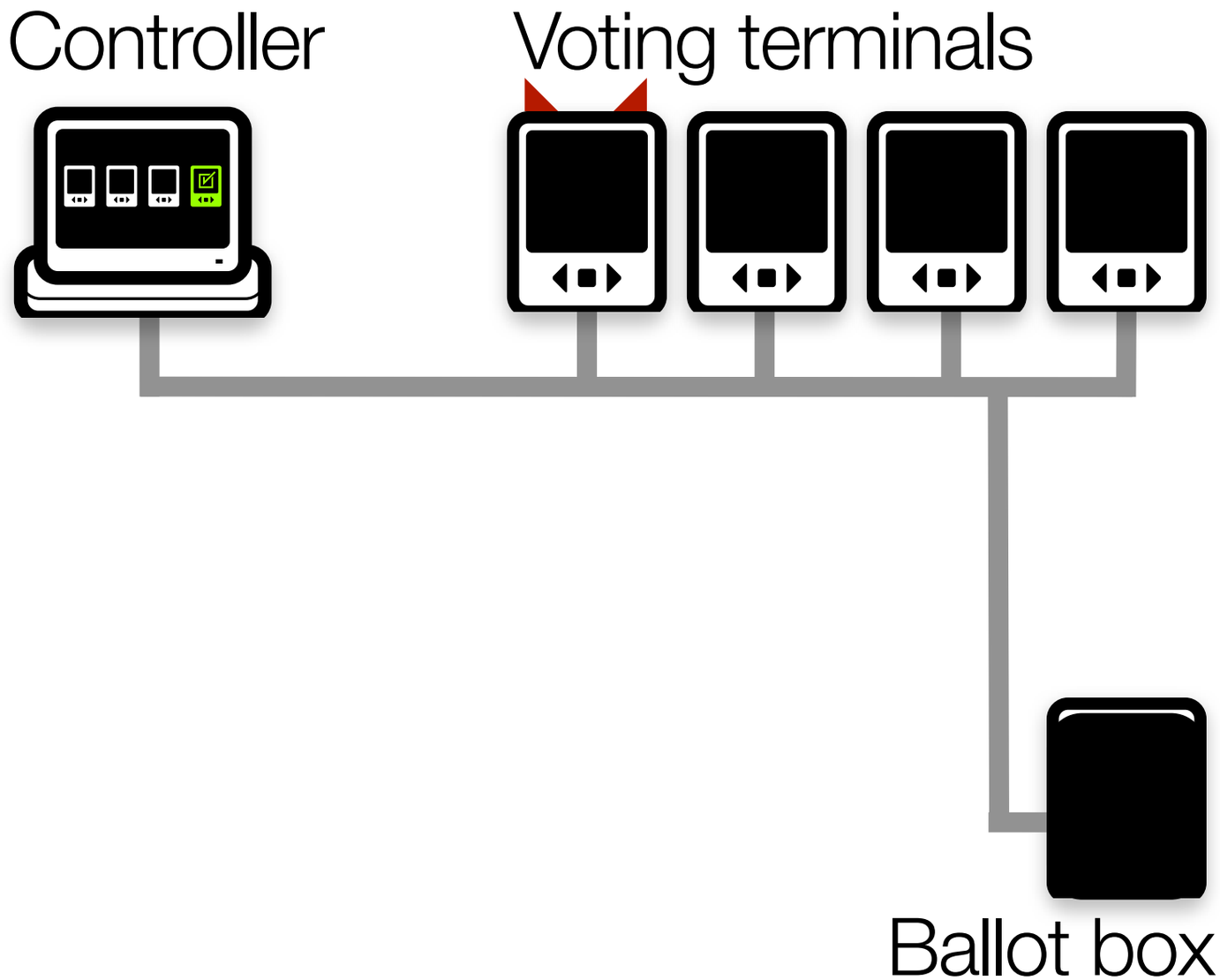
Forged votes on one device?

Trivially detectable

No matching authorizations

Voting terminal can’t forge because it doesn’t have controller’s public key

No matching paper ballots



Conspiracy with controller?

Votes recorded everywhere?

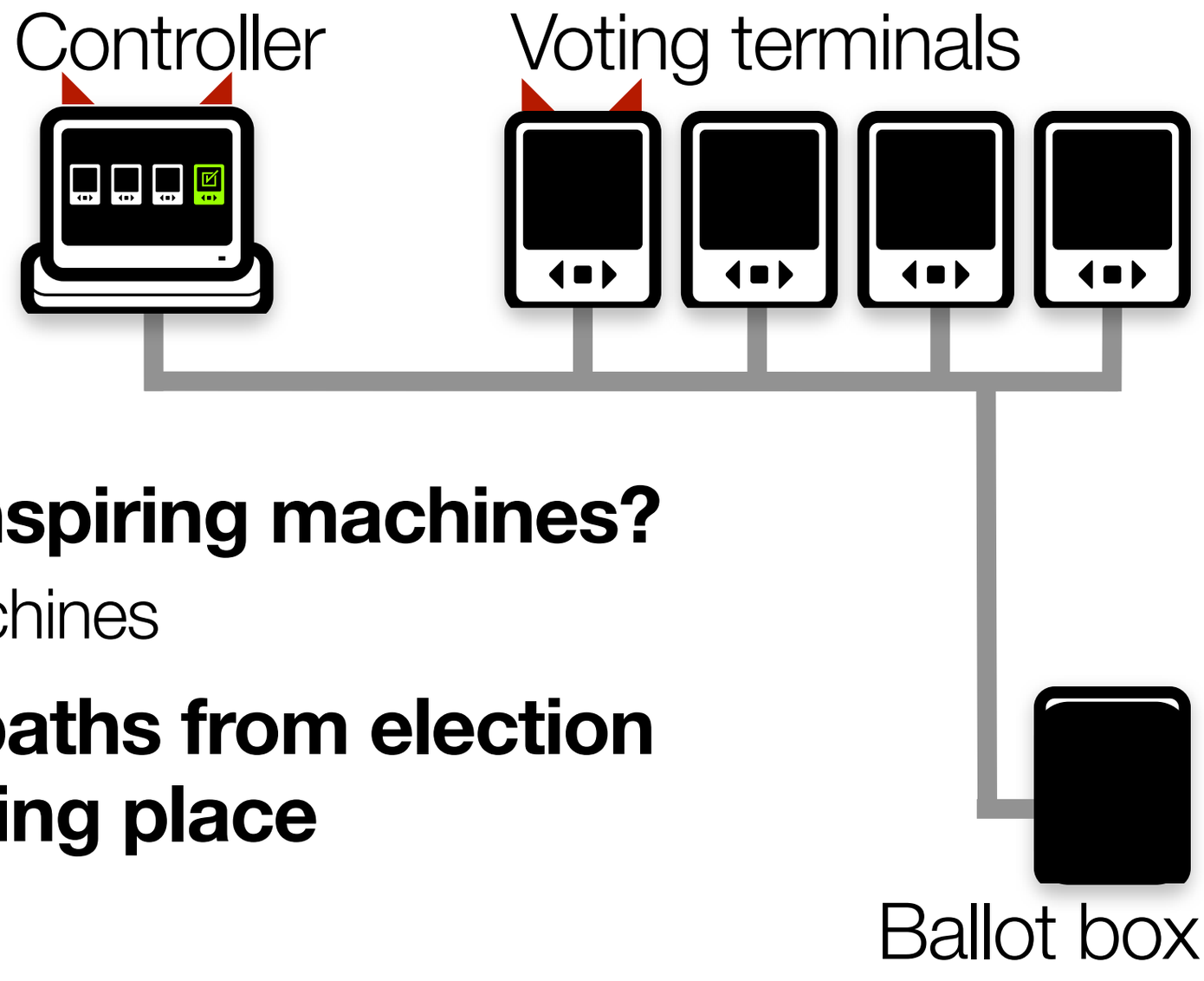
Inconsistent with paper

Inconsistent with registration data

Recorded only on conspiring machines?

Inconsistent with good machines

Mitigation: Separate paths from election warehouse to the polling place



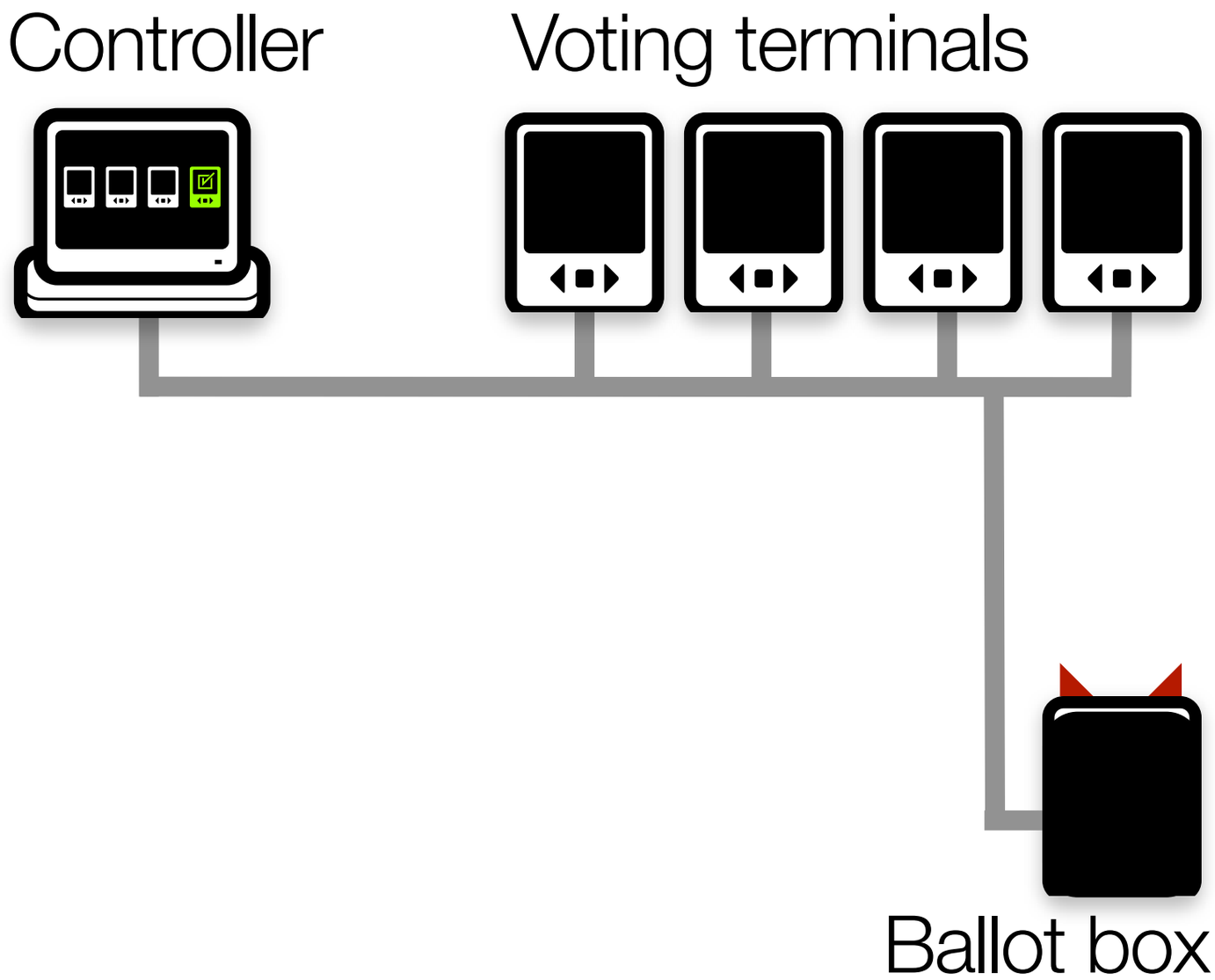
Paper ballot stuffing?

Primary tallies use electronic ballots

Paper without corresponding ciphertext is suspicious

Chain voting

Detect/reject based on timestamps



Malicious machine? (integrity)

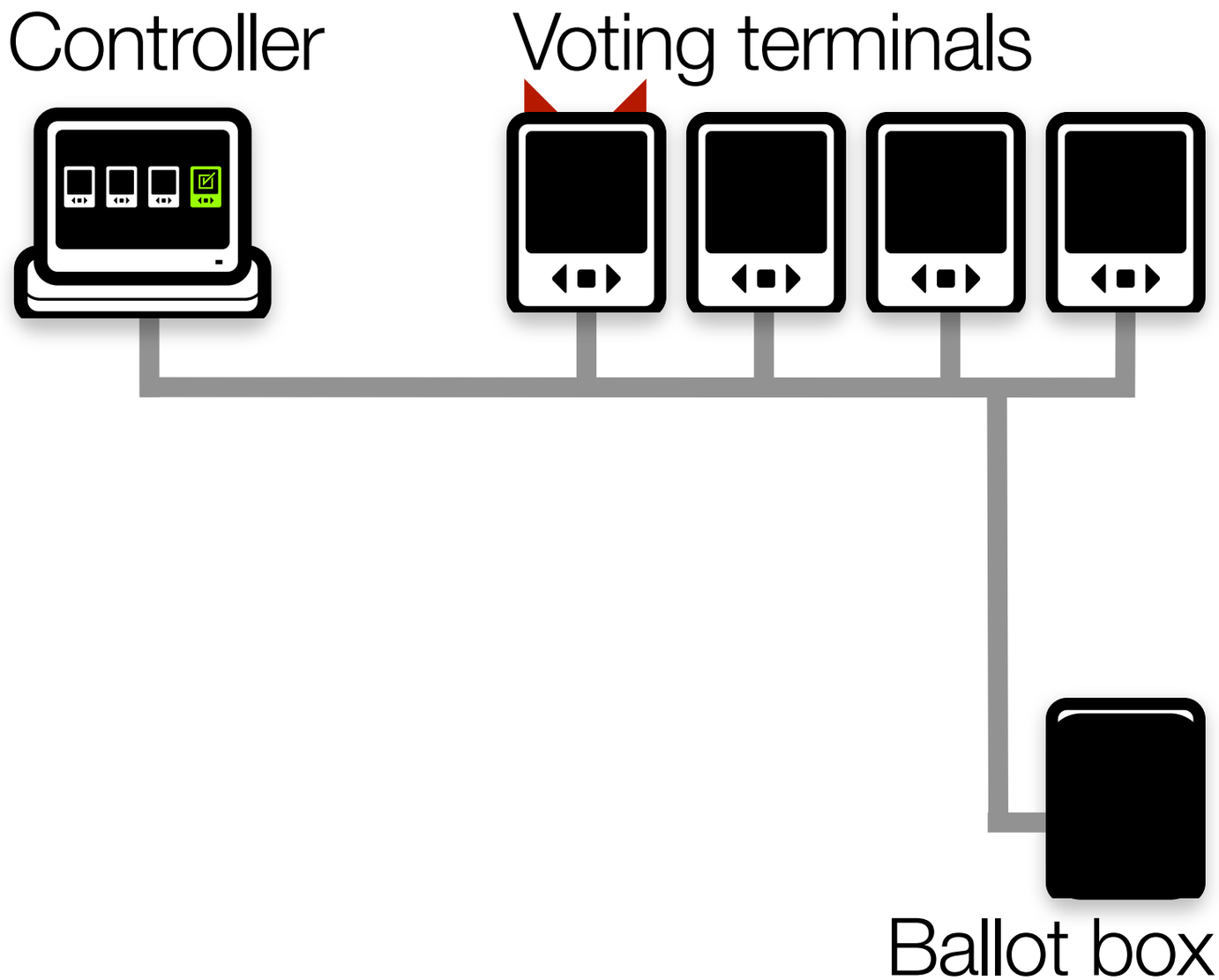
Show A, record B

Paper ballot inconsistent with ciphertext ballot

Two ways to detect

Post-election audit (compare paper to decrypted ciphertexts)

Benaloh-style challenge

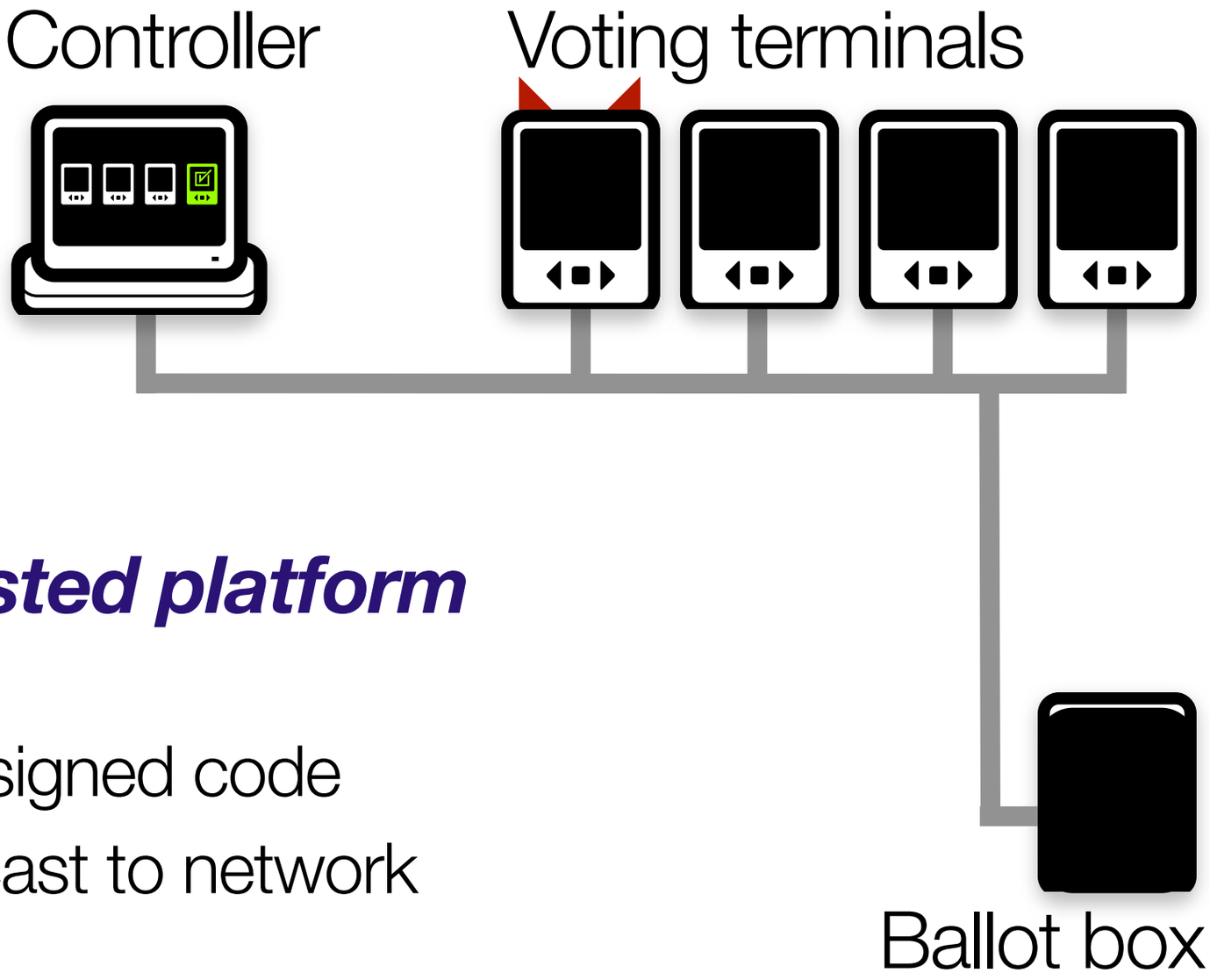


Malicious machine? (privacy)

Record plaintext ballots in order cast

(or *subliminal channels*)

Fundamental problem!



Tentative solution: *trusted platform management* (TPM)

Terminals refuse to boot unsigned code

Integrity attestations broadcast to network

Malicious / offline ballot box

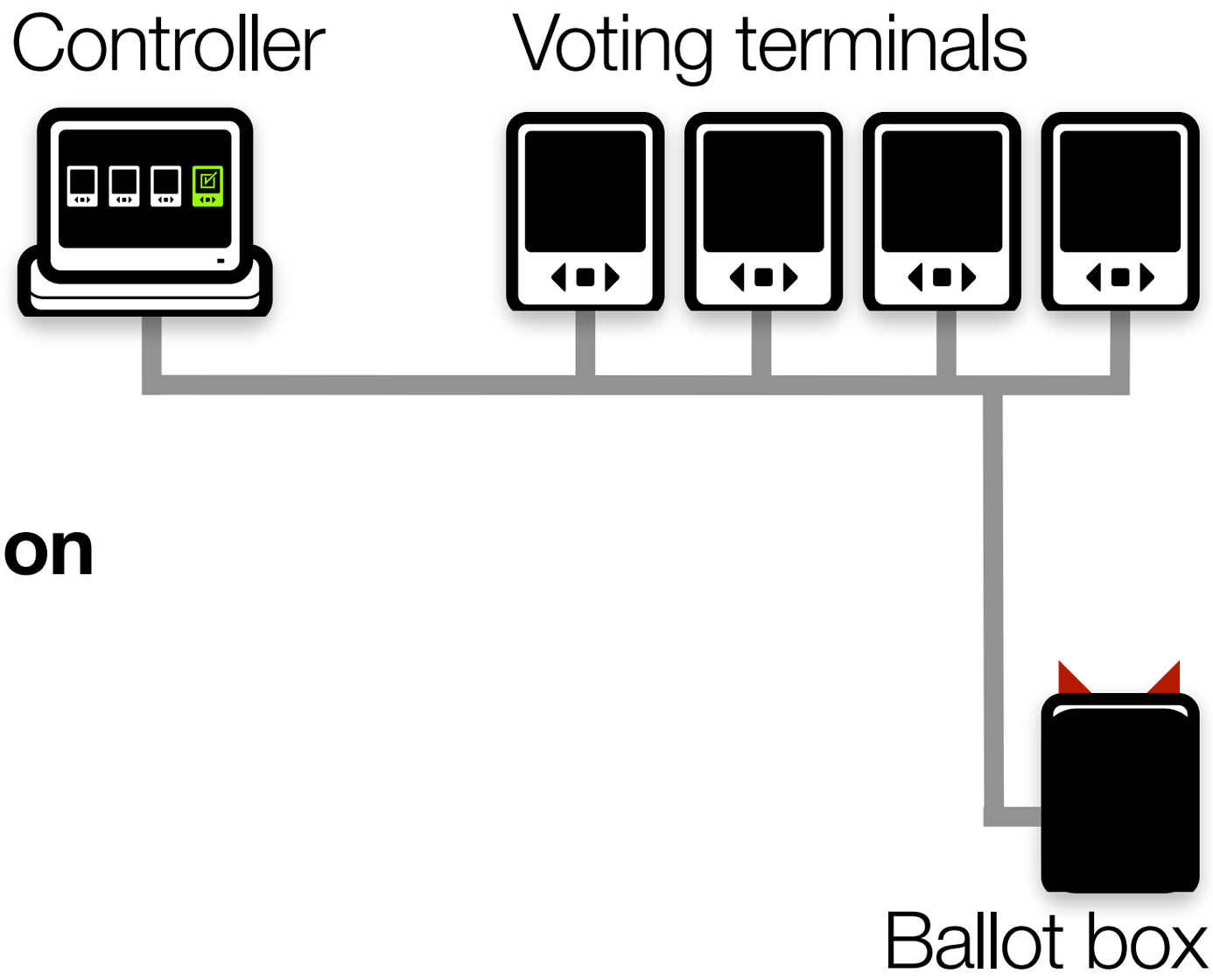
No ballot acknowledgements

Observable by controller

Warn poll workers

Election-night resolution

Rescan deposited ballots



Coerce voter w/ ballot randomness?

E.g., “cast if even, challenge if odd.”

Voter can deliberately spoil and revote many times (“oops!”)

Stronger mitigations possible (e.g., don’t print textual hashes, only barcode)

Bad impact on usability



Voter presents “fake” receipt

Falsely impugn the election?

Possible mitigations:

- Watermarking on physical paper
- Digital signature within QRcode

Similar issues with challenge ballots

Ballot spoiling process can include wet signatures of poll workers

YOUR VOTE COUNTS

Thank you for voting!

Take this confirmation of voting with you

Verify your ballot at:

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

Voting Date: October 30, 2012
Voting Terminal: UI12345

Location: Randall's South Mopac
Time: 18:45:56

Status

VoteBox-based proof-of-concept in progress

Production system would want to start from scratch

Design mostly set

RFP almost ready to launch

Legalities?

Federal and state certification processes

STAR-Vote is nothing like any other certified voting system

Probably needs to get waivers or amend laws

What's "the ballot"?

We've got lots of copies

Depending on what fails, one might be better than another

"Best record of voter intent" might be a better phrase

What's a "recount"?

We've got lots of evidence

Some is easy to examine mechanically (and will be, regardless)

Other stuff requires manual analysis

Maybe "risk limiting audit with large sample size" might work

Practicalities?

Provisional voting

Perhaps have voter use web-based UI to fill out forms

Printed ballot goes in envelope, not ballot box

Ciphertext ballot marked as provisional

Anonymity of provisional voters' preferences preserved

"Limited" ballots

Voter moves to Travis from adjacent county, hasn't re-registered

Voter gets a ballot with only overlapping races

Write-in votes

In Texas, write-in candidates must register in advance

Should we help the voter select a registered write-in?

Extension #1: remote voting

If the data formats were standard...

Ballot style definitions

Encrypted vote output

... then we could ship ballot definitions anywhere

Embassies, consulates, military bases

... and return the encrypted ballots electronically

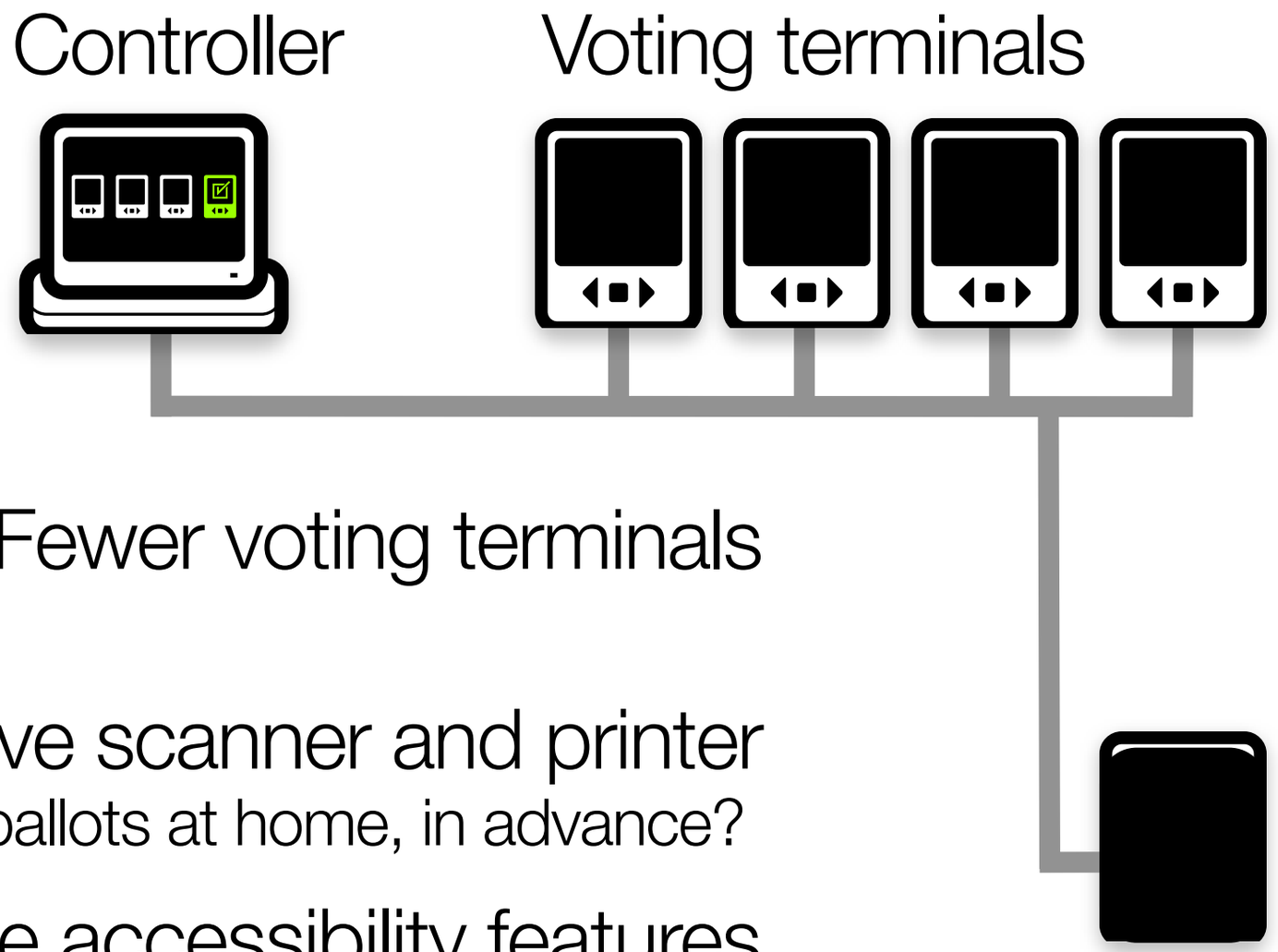
With the paper ballots to follow via courier services

Handling would be similar to provisional votes

(Note: remote voting ≠ Internet voting)

Extension #2: Hand-marked paper

If an election authority didn't have Travis County's constraints



Fewer voting terminals

New terminals have scanner and printer

Fill out "draft" ballots at home, in advance?

Same accessibility features

Identical back-end processing

Non-profit consortium?

If this works for Travis, it could work for others

Other counties could pitch in

Consortium can share costs over a larger community

Some counties already do this for other functions (e.g., records management), so the business model is understood

Vendors can resell hardware, offer training, support contracts

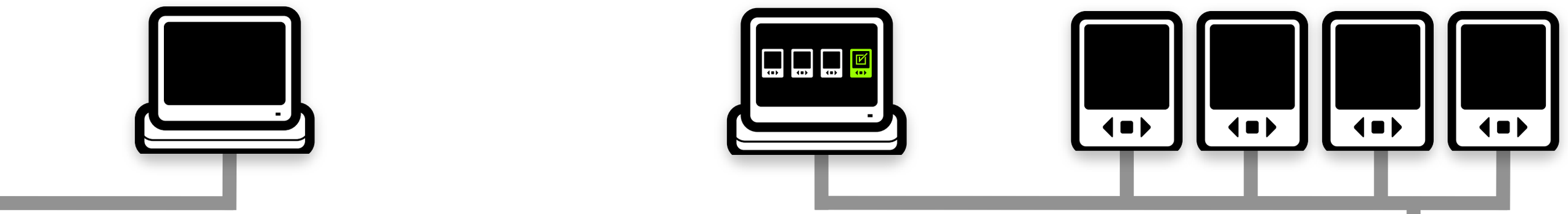
Open source?

STAR-Vote: It's happening

Registration

Controller

Voting terminals



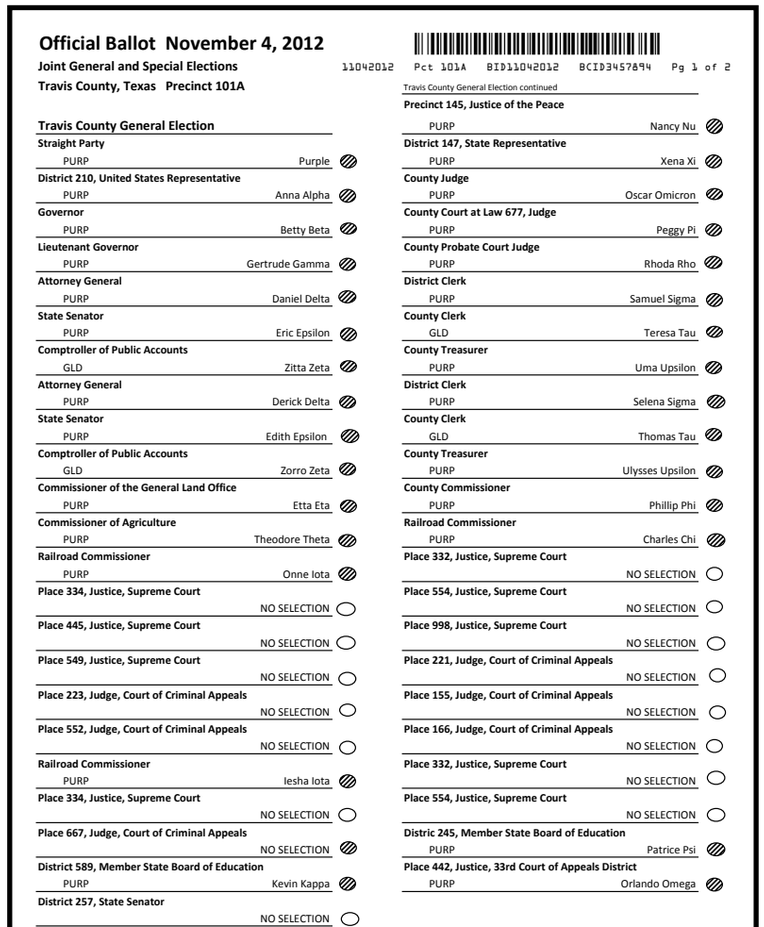
E2E verification

Risk-limiting audits

Tons of redundancy

Usability/accessibility

COTS hardware



Official Ballot November 4, 2012

Joint General and Special Elections 11042012 Pct 101A BID11042012 BCID3457894 Pg 1 of 2

Travis County, Texas Precinct 101A

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

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

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

Distric 245, Member State Board of Education
PURP — Patrice Psi

Place 442, Justice, 33rd Court of Appeals District
PURP — Orlando Omega

Ballot box