

Asynchronicity and Revoting in Helios

Susan Thomson, University of Bristol
Based on joint work with Ben Smyth, Huawei

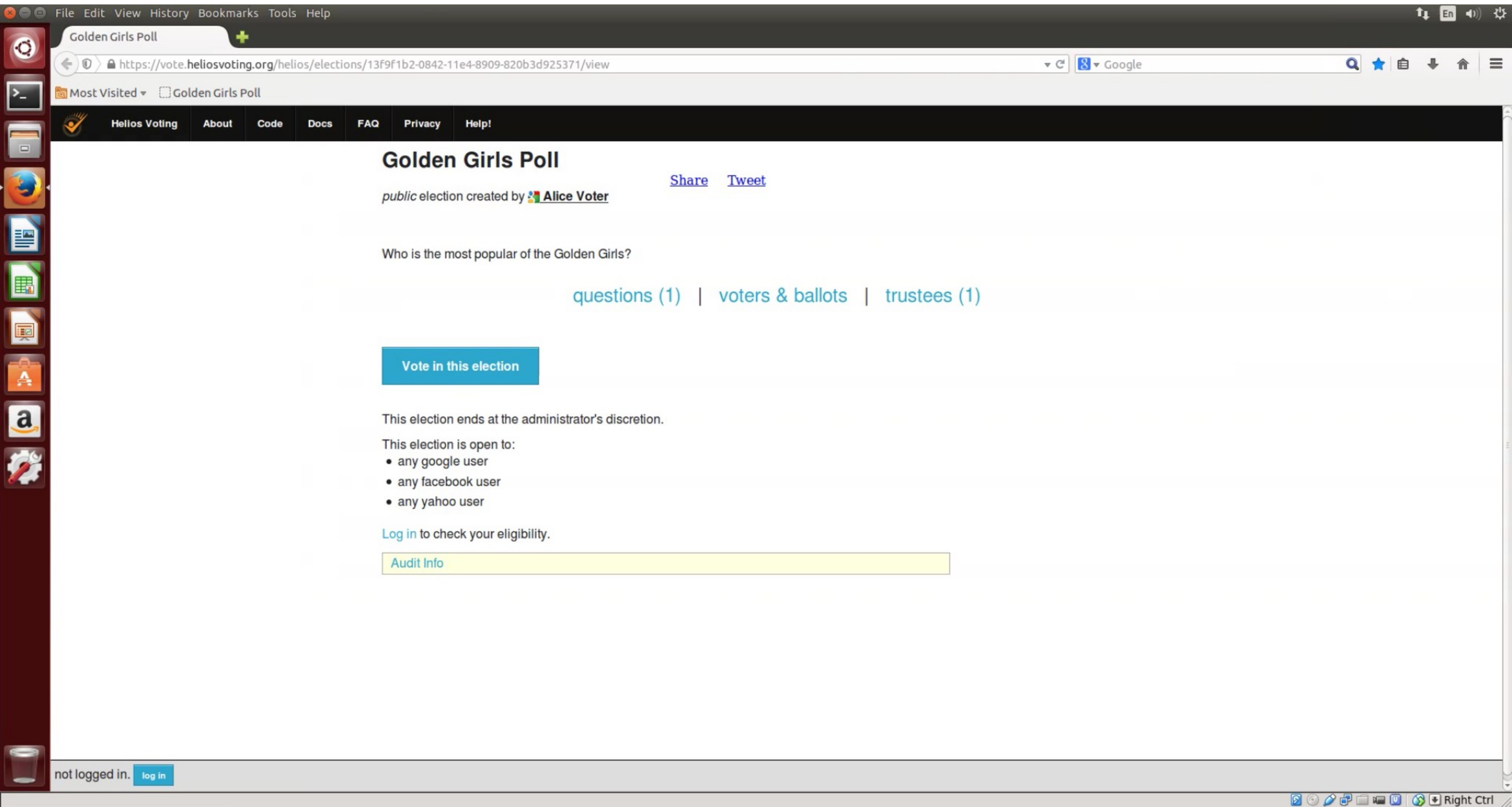
Election 2015: Leaders set out rival 'choices'

🕒 1 hour ago | [Election 2015](#) | 💬 2123



helios

Trust the vote.



Helios Voting Booth

[\[exit\]](#)

Golden Girls Poll

To cast a vote, you will be led through the following steps.
If you have not yet logged in, you will be asked to do so at the very end of the process.

1. **Select** your preferred options.
You can easily navigate forwards and backwards.
2. **Review & Confirm** your choices.
Your choices are encrypted safely inside your browser, and you get a smart ballot tracker.
3. **Submit** your encrypted ballot.
You will be asked to log in to submit your encrypted ballot for tallying.

[Start](#)Election Fingerprint: **EaJTv8KC2bpXy9LZ0YopvwmQDbjqtXu0cJGz6AkRNhc**[help!](#)

Helios Voting Booth

[\[exit\]](#)

Golden Girls Poll

(1) Select

(2) Review

(3) Submit

Choose your favourite of the Golden Girls

#1 of 1 — vote for 1

- ☐ Blanche
- ☐ Dorothy
- ☐ Rose
- ☐ Sophia

Proceed

Election Fingerprint: EaJTv8KC2bpXy9LZ0YopvwmQDbjqtXu0cJGz6AkRNhc

[help!](#)

Helios Voting Booth

[\[exit\]](#)

Golden Girls Poll

(1) Select

(2) Review

(3) Submit

Choose your favourite of the Golden Girls

#1 of 1 — vote for 1

- ☐ Blanche
- ☒ Dorothy
- ☐ Rose
- ☐ Sophia

Proceed

Election Fingerprint: EaJTv8KC2bpXy9LZ0YopvwmQDbjqtXu0cJGz6AkRNhc

[help!](#)

Helios Voting Booth

[\[exit\]](#)

Golden Girls Poll

(1) Select

(2) Review

(3) Submit

Review your Ballot

Choose your favourite of the Golden Girls

Dorothy [\[edit\]](#)

Confirm Choices and Encrypt Ballot

Election Fingerprint: **EaJTv8KC2bpXy9LZ0YopvwmQDbjqtXu0cJGz6AkRNhc**

[\[help!\]](#)

Helios Voting Booth

[\[exit\]](#)

Golden Girls Poll

(1) Select

(2) Review

(3) Submit

Your ballot is ready to be submitted

Don't forget to click "Proceed to Submission" below!

Before submitting, you can take note of your smart ballot tracker [\[print\]](#):

Ysyb2TK7Xr1sfs80DAYsbm50vncvY7cspjlnGDEV4K8

Once you click "Proceed", Helios will remember only your encrypted vote. Thus, only you know your vote.

[Proceed to Submission](#)[Audit](#) [optional]

Election Fingerprint: **EaJTv8KC2bpXy9LZ0YopvwmQDbjqtxu0cJGz6AkRNhc**

[help!](#)



Golden Girls Poll — Submit your Vote

We have received, **but not yet recorded**, your encrypted ballot.
Your smart ballot tracker is:

Ysyb2TK7Xr1sfs80DAYsbm50vncvY7cspjlnGDEV4K8

Now, we need you to log in, so we can verify your eligibility.



yahoo



facebook



google

Don't worry, we'll remember your ballot while you log in.



Sign in with your Google Account



votercharlie@gmail.com

.....

Sign in

☒ Stay signed in

[Need help?](#)

[Create an account](#)

One Google Account for everything Google






Golden Girls Poll — Submit your Vote

We have received, **but not yet recorded**, your encrypted ballot.
Your smart ballot tracker is:

Ysyb2TK7Xr1sfs80DAYsbm50vncvY7cspjlnGDEV4K8

You are logged in as  [Charlie Voter](#)

CAST this ballot

You can cast as many ballots as you want.
Only the last one counts.

cancel

If you cancel now, your ballot will *NOT* be recorded.
You can start the voting process over again, of course.



Golden Girls Poll — Vote Successfully Cast!

Congratulations, your vote has been successfully cast!

Your smart ballot tracker is:

Ysyb2TK7Xr1sfs80DAYsbm50vncvY7cspjlnGDEV4K8

[Share](#) [Tweet](#)

For your safety, we have logged you out.

[\[return to election info \]](#)

Generate ballot

Confirm Choices and Encrypt Ballot



Authenticate ballot

Sign in



Process ballot

CAST this ballot

Voting scheme syntax

- Setup \rightarrow private info x , public info y , bulletin board BB
- Vote(choice of candidate c) \rightarrow ballot b
- Auth(b , identifying information id) \rightarrow tag t
- ProcessBallot(BB, b , t) \rightarrow updated BB
- Tally(BB, x) \rightarrow result $p(\text{votes } V)$

Simple voting scheme

- Setup \rightarrow blank private info x , public info candidate list, bulletin board BB
- Vote(choice of candidate c) \rightarrow ballot b is c
- Auth(b , voter's name id) \rightarrow tag t is id
- ProcessBallot(BB, b , t) \rightarrow append (c, id) to BB if $(*,id)$ does not appear on BB
- Tally(BB, x) \rightarrow most common c on BB

CORRECTNESS

$(x, y, BB) \leftarrow \text{Setup}$

$\perp \leftarrow A^{\text{VOTE}}(y)$

if ($\text{Tally}(x, BB) \neq \rho(V)$)

 return 0

return 1

proc VOTE(c, id)

$b \leftarrow \text{Vote}(c)$

$t \leftarrow \text{Auth}(b, id)$

if ($V[id] = \perp$)

$V[id] \leftarrow c$

ProcessBallot(BB, b, t)

return



Vote with help

Revote later in private



Ballot processing with revoting

ProcessBallot(BB, b, t):

- If t is on BB, overwrite (*,t)
- Otherwise append (c, id) to BB

CORRECTNESS

$(x, y, BB) \leftarrow \text{Setup}$

$\perp \leftarrow A^{\text{VOTE}}(y)$

if ($\text{Tally}(x, BB) \neq \rho(V)$)

 return 0

return 1

proc VOTE(c, id)

$b \leftarrow \text{Vote}(c)$

$t \leftarrow \text{Auth}(b, id)$

if ($V[id] = \perp$)

$V[id] \leftarrow c$

if (revoting = true)

$V[id] \leftarrow c$

ProcessBallot(BB, b, t)

return





Network

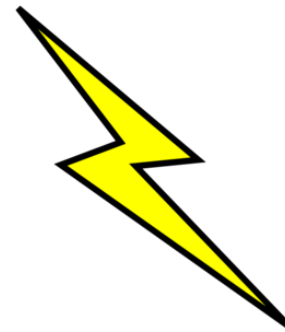
helios
Trust the vote.



CAST this ballot



CAST this ballot





CORRECTNESS

$(x, y, BB) \leftarrow \text{Setup}$

$A^{\text{VOTE}, \text{RECORD}}(y)$

if $(\text{Tally}(x, BB) \neq \rho(V)) \wedge (G = R)$

 return 0

return 1

proc VOTE(c, id)

$b \leftarrow \text{Vote}(c)$

$t \leftarrow \text{Auth}(b, id)$

if $(V[id] = \perp)$

$V[id] \leftarrow c$

if (revoting = true)

$V[id] \leftarrow c$

$G \leftarrow G \cup \{(t, b)\}$

return b

proc RECORD(b, t)

if $((t, b) \in G)$

$R \leftarrow R \cup \{(t, b)\}$

 ProcessBallot(BB, b, t)

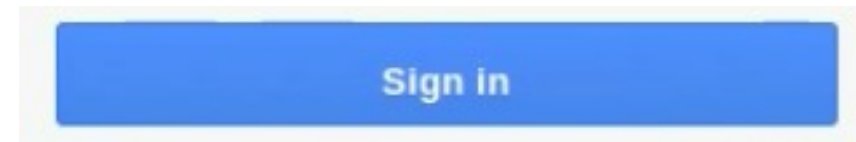
return

Generate ballot

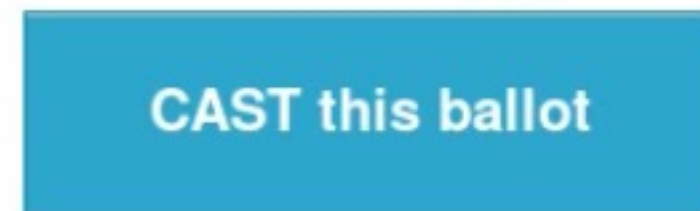
Confirm Choices and Encrypt Ballot



Authenticate ballot



Process ballot



Time stamped ballot processing

ProcessBallot(BB, b, t):

- if t is on BB with earlier time stamp, overwrite (*,t)
- if t is on BB with later time stamp do nothing;
- otherwise append (c, id) to BB



Network

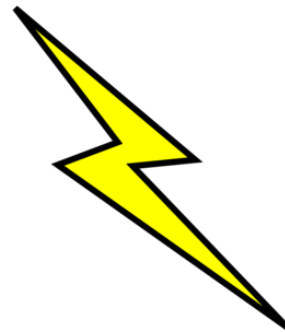
helios
Trust the vote.



CAST this ballot



CAST this ballot



Conclusions



Time is important in a
network protocol



Time is hard to
model