Securing the Foundations of Democracy

Peter Y A Ryan

Université du Luxembourg

Democracy in Crisis

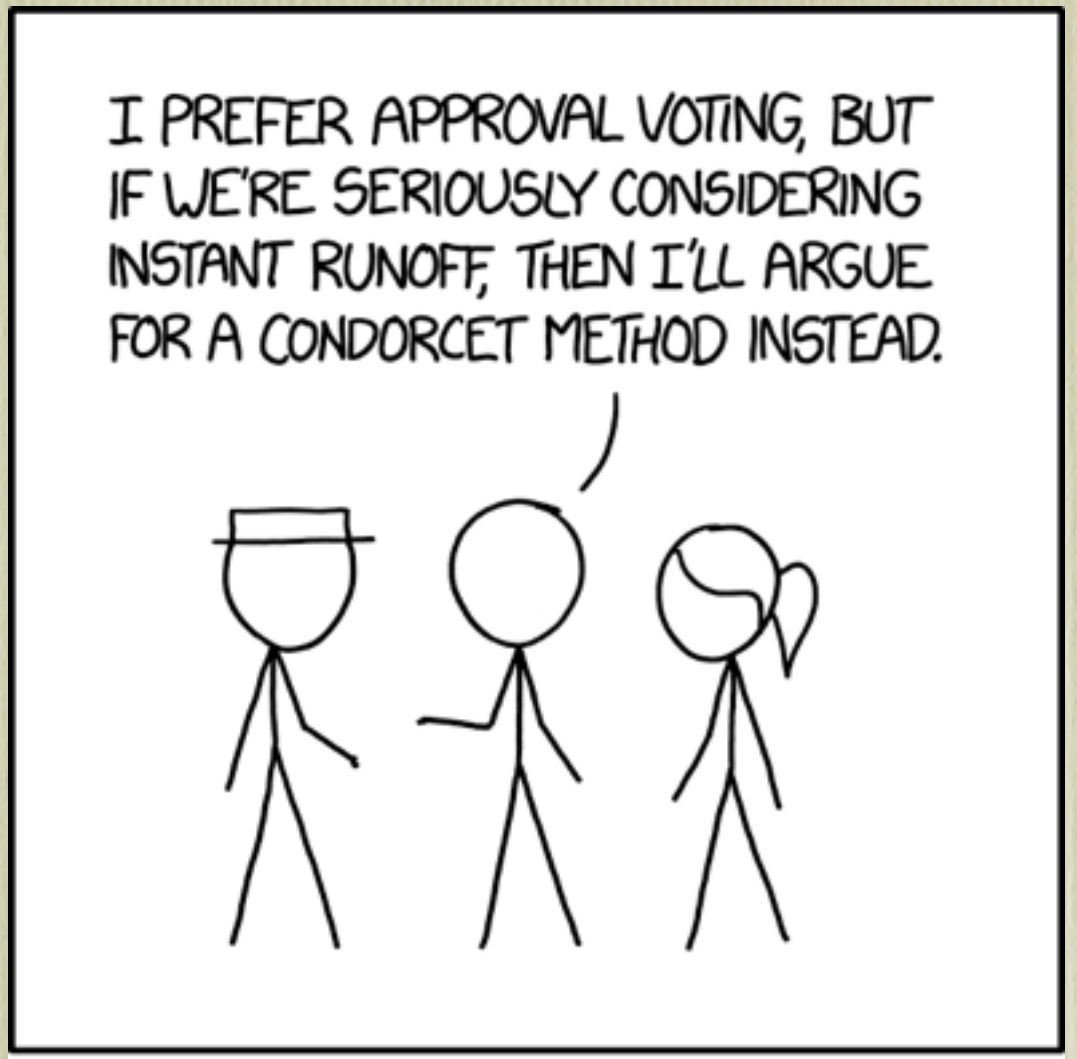
- Digitisation of democracy holds out great promise but also brings new and major threats.
- We have witnessed several spectacular failures of democracy recently, and are in danger of more soon.
- Allegations of Russian interference in US election.
- Evidence of hacking of voter registration DBs.
- And of the Democratic campaign.

Democracy in Crisis

- No proof of tampering with votes, but attempts to recount in Pennsylvania, Wisconsin and Michigan. Largely blocked either technically or legally.
- “Alternative” news, information bubbles.
- Chilling effect of mass surveillance
- Here I will focus just on securing the casting and counting of votes.

Democracy in crisis

- “These truths are self-evident, but not self-enforcing.” Barak Obama
- Elections part of the national critical infrastructure!?



STRONG ARROW'S THEOREM: THE PEOPLE WHO FIND ARROW'S THEOREM SIGNIFICANT WILL NEVER AGREE ON ANYTHING ANYWAY.

Possible responses

- Go back to paper ballots and hand counting.
- Ensure that meaningful audits can be performed, e.g. VVPAT, Risk Limiting Audits (Stark et al) etc.
- End-to-end verifiable schemes.
- Hybrid schemes.

Trust

- Trust in the process and the outcome is paramount.
- Elections should be evidence-based.
- Traditional voting requires a high degree of trust.
- Touch screen voting requires blind trust-How many Diebold technicians does it take to change an election?
- “Trustworthiness before trust”, Baroness Onora O’Neill.

And mistrust!

Lever machines

- 

Op-scan ballot

Touch-screen

- 

Punch Card

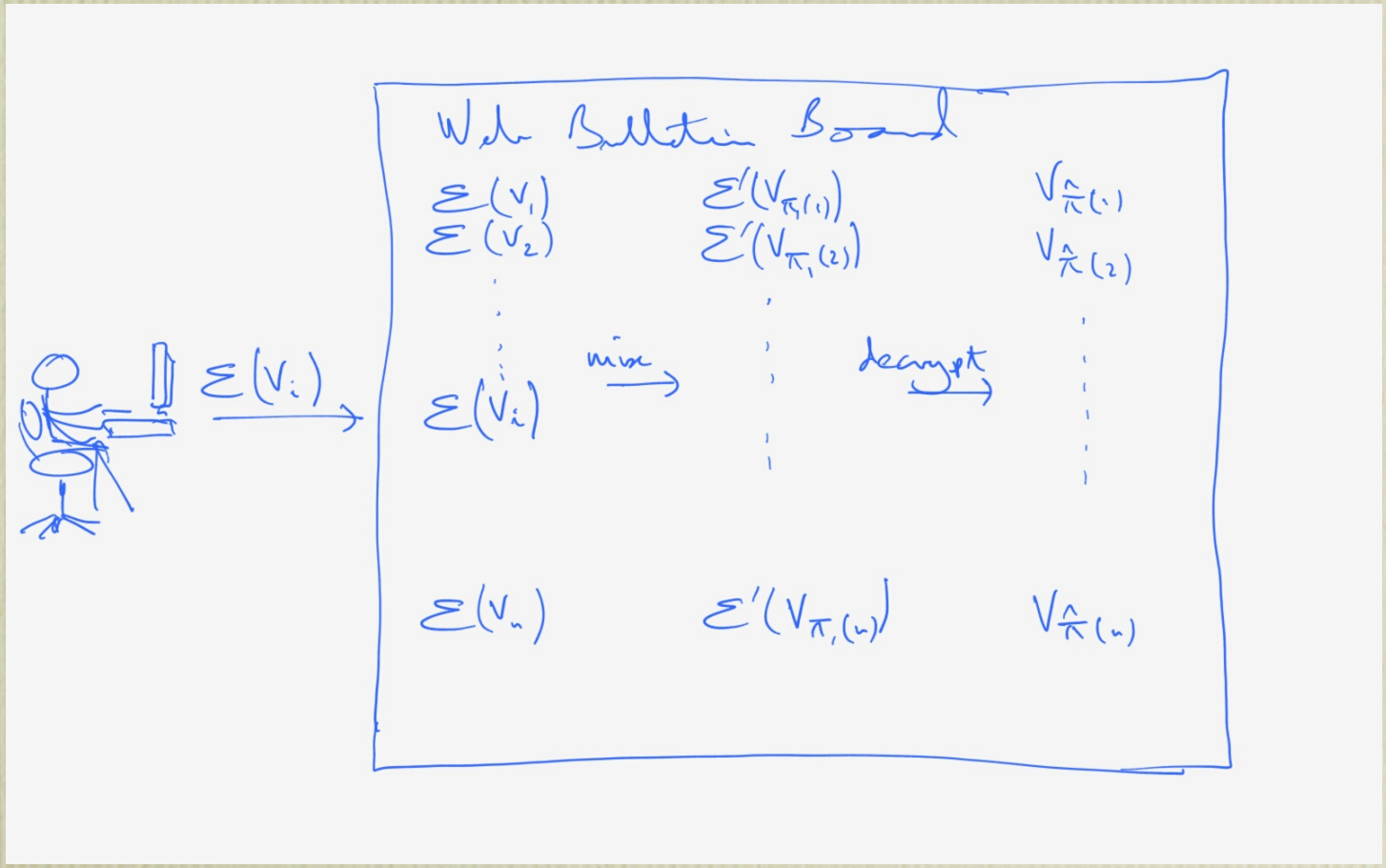
The Challenge

- The correctness of the outcome of an election should be universally demonstrable, while ensuring ballots remain private.
- No god's eye view of the correct answer!
- We need to resolve the tension between verifiability and ballot secrecy.
- Either alone is trivial but achieving both together, **without trusted parties,** is immensely challenging.

E2E Verifiability

- Goal: voters can confirm that their vote is accurately counted, but without introducing coercion threats.
- Assurance by the people for the people!
  - At the time of casting voters get an encrypted/encoded representation of their vote.
  - Cast receipts are posted to a secure web bulletin board (WBB). Voters can verify that their receipt is correctly posted.
  - A (universally) verifiable, anonymising tabulation is performed on the posted receipts.

Public Bulletin Board



The assurance argument

- Each voter must be confident that her/his vote is correctly encrypted.
- We need to be sure that all legitimately cast (encrypted) votes are input to the tally (on the WBB).
- We need to be sure that this set of encrypted votes is correctly anonymised and decrypted.

Assurance

- The really tricky bit is the first: how to convince the voter without creating proof to a coercer.
- E2E V schemes typically depend on a reasonable numbers of voters performing checks.
- The third aspect is fairly standard crypto-maths.

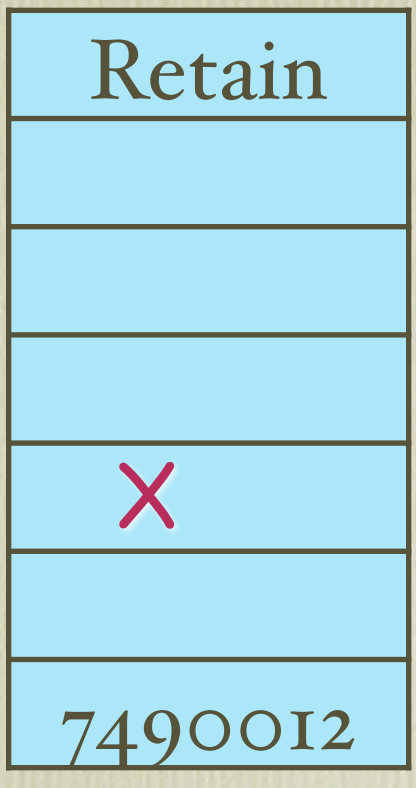
Prêt à Voter

- Uses familiar, paper ballot forms.
- But the candidate list is independently randomized on each ballot form!
- Information defining the candidate order is encrypted on the ballot.
- After marking her choice, X or ranking etc, the candidate list is detached and shredded.

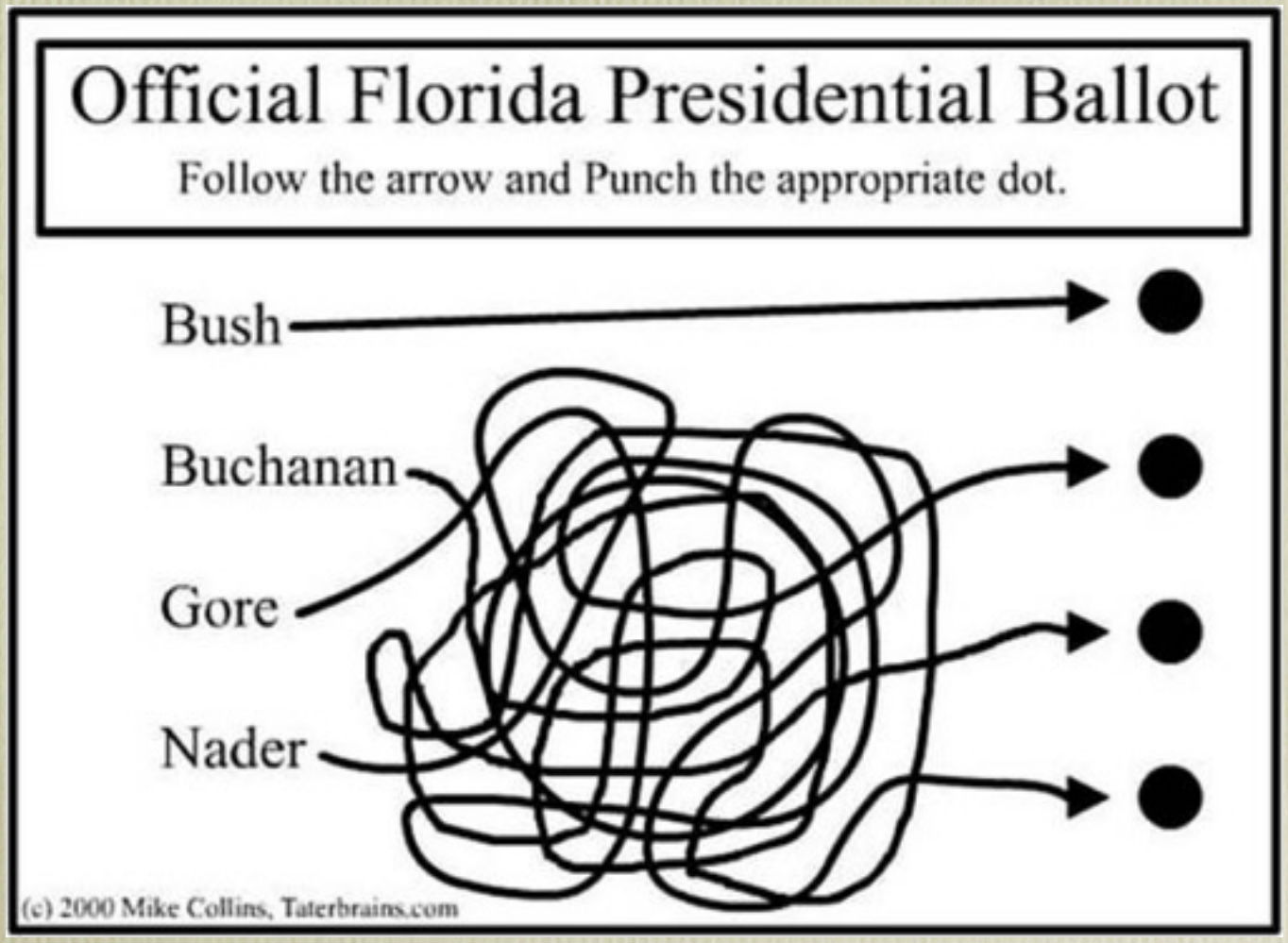
Prêt à Voter Ballot

Destroy	Retain
Asterix	
Obelix	
Idefix	
Panoramix	X
Abraroucourix	
	7490012

Prêt à Voter Ballot



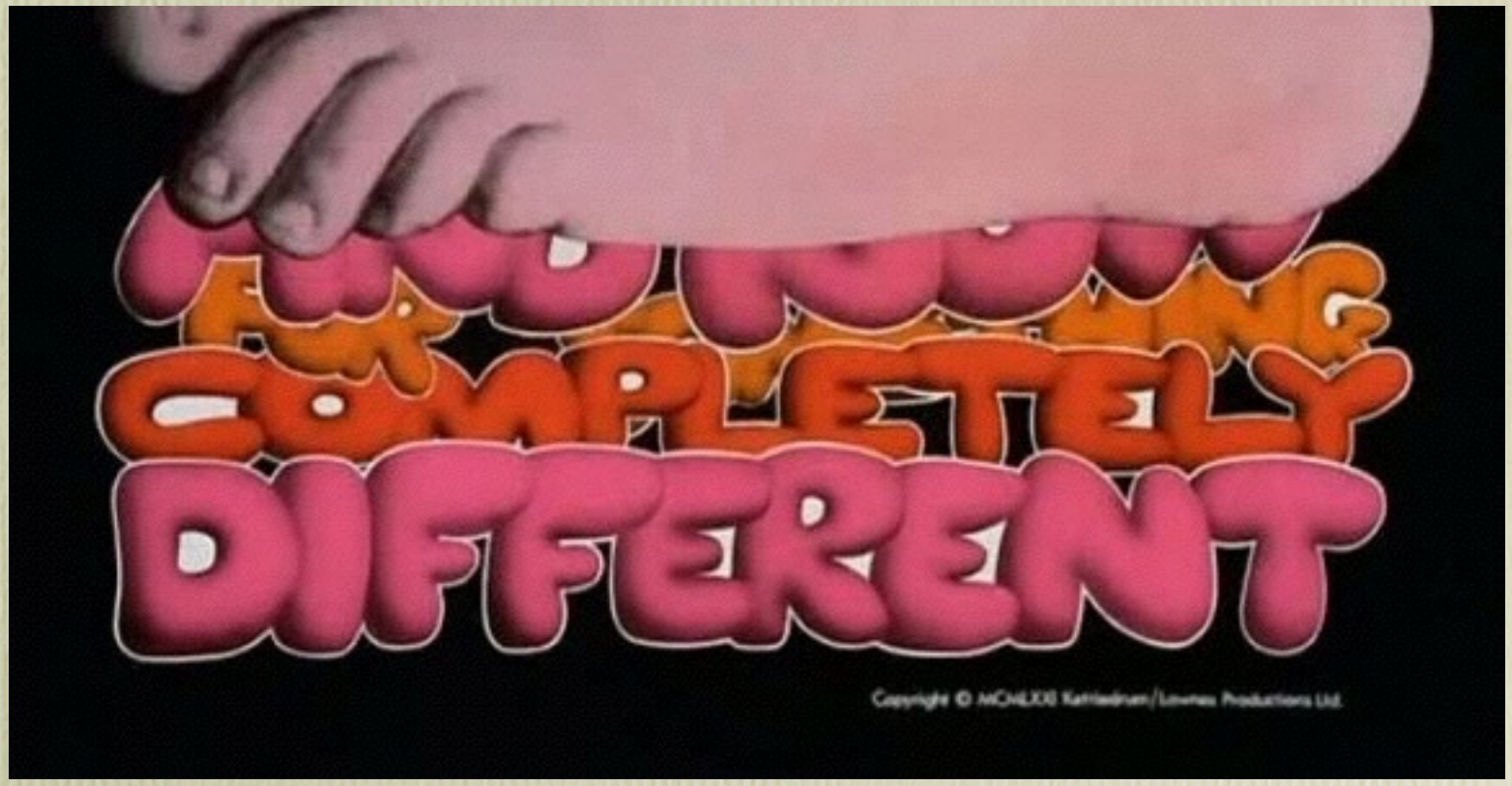
Inspiration!?



Remarks

- The receipt reveals nothing about the vote
- Voter experience simple and familiar.
- Voters do not communicate their choice to a device, (neatly sidesteps many side-channel threats).
- Cast as intended <=> wellformedness of the ballot.
- Ballot auditing rather clean w.r.t. privacy and dispute resolution.
- Can be adapted to deal with ranked voting, Approval Voting etc.

And now.....



Voter-friendly Verification

- All very nice but....
- But try selling this to an election official!
- Voter verification steps can be burdensome and non-intuitive.

Vote Trackers

- A very simple approach: give each voter a private tracker number and post these on the WBB alongside the vote in the clear.
- Verification is simple and intuitive-no need to handle encrypted ballots etc.

Tracker numbers

347563	Obelix
947253	Asterix
556884	Panoramix
569331	Idefix
586994	Idefix
607855	Obelix
374823	Obelix

But....

- We have to guarantee that voters get unique trackers.
- Seems wide open to coercion.
- Largely ignored by the crypto/security community, aside maybe for “boardroom” style contexts.

Coercion Attack

- Coercer requires the voter to reveal her tracker number so that he can check how she voted.
- However: the coercer has to require the voter to reveal her tracker before the ballots are posted. Otherwise the voter just pulls a suitable tracker off the WBB.
- So what if voters only learn their number after the votes and trackers have been posted!?

The goals of Selene

- To ensure that each voter is assigned a unique tracker number.
- To notify the voters of their trackers (after trackers/votes pairs have been posted) in a way that provides high assurance but is deniable.
- And we want to do this in a way that ensures no single entity knows the assignment.

The Setup

- For each voter we want to post to the WBB:
- $PK_i, \{n_i\}_{PK}, TDC_i\{n_i\}$
- $\{n_i\}_{PK}$ will be used in the tabulation.
- $TDC_i\{n_i\}$, Trap Door Commitment for voter i, will be used in notifying the voter of the tracker.

Set-up

- Generate sufficient tracker numbers n_i and post the list to the WBB.
- Form (ElGamal) encryption under the Teller's PK of the n_i : $\{n_i\}_{PK}$.
- Put these through verifiable re-encryption mixes and assign the resulting shuffled, re-encrypted numbers to the voters' Ids (PK_i).
- PK_i:, $\{n_{\pi(i)}\}_{PK\_T}$

Set up

- Now we use a distributed construction to transform the $\{n_{\pi(i)}\}_{PK}$ into the trapdoor commitment $n_{\pi(i)} \cdot h_i^{r_{-i}}$
- $n_{\pi(i)} \cdot h_i^{r_{-i}}$ is voter i's trapdoor PK.
- On the WBB we now have rows of the form:
- $PK_i, \{n_{\pi(i)}\}_{PK}, n_{\pi(i)} \cdot h_i^{r_{-i}}$
- Ready for the i-th voter 's ballot.

Voting

- To vote, the voter forms:
- $$\mathrm{Sig}_{V_i}(\{|\mathrm{Vote}_i|\}_{PK})$$
- This is posted to the appropriate row of the WBB:
- $$PK_i, \{n_{\pi(i)}\}, n_{\pi(i)} \cdot h_i^{r_{-i}}, \mathrm{Sig}_{V_i}(\{|\mathrm{Vote}_i|\}_{PK})$$
- Proofs and signatures are checked, invalid ballots discarded.

Tabulation

- We extract the last two terms of the tuple, and strip off the signature and ZK proofs:
- $(\{n_{\pi(i)}\}_{PK}, \{Vote_i\}_{PK})$
- These are now put through verifiable, parallel, re-encryption mixes and threshold decrypted:
- $(n_{\pi(i)}, Vote_i)$

Notifying the trackers

- Trustees reveal g^{r_i} to the i-th voter through a private (anonymous) channel.
- The voter can now form the ElGamal cryptogram:
- $$(g^{r\_i},\ h_i^{r\_i,} \cdot n_{\pi(i)})$$
- which she can decrypt as usual with her secret key x_i to reveal: $n_{\pi(i)}$.

Coercion Resistance

- If V_i is coerced she can compute, with knowledge of the trapdoor, an alternative $(g^{r\_i})'$ value which will open the encryption to whichever tracker number she needs to satisfy the coercer.
- On the other hand, without the knowledge of secret trapdoor, this is intractable, so revealing the wrong tracker to the voter is intractable for an attacker.

Conclusions

- Digitisation of democracy holds out great promise but also brings great dangers.
- E2E V schemes hold out promise.
- A lot of snake oil out there.
- Currently no known way to make internet voting sufficiently secure for binding, political elections.
- Securing democracy is immensely challenging, but absolutely fascinating.

Thank you!

Credits

- Josh Benaloh David Chaum, Ron Rivest, Alon Rosen, Philip B Stark, Joson Zia.
- On location in Australia:
- Special thanks to: Craig Burton, Chris Culnane, James Heather, Steve Schneider, Vanessa Teague.
- Fonds Nationale de Research (FNR) Luxembourg.