How a Crypto Protocol Can Ensure Free and Fair Elections

Bernard Fickser

Expensivity.com

Nancy is an eligible voter.

Nancy wants to vote in a free and fair election.

The election is between Alice and Bob.

Alice

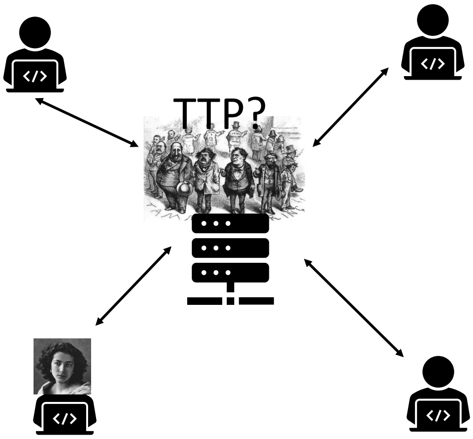
Bob

Nancy is worried about the election commission.

The election commission has a history of being at best lax, at worst corrupt.

Should Nancy trust third parties like the election commission?

No, all third parties can as easily make promises as break their promises and prove untrustworthy. Nancy, to be confident that her vote is being counted, must be able to ensure that her ballot is counted in spite of third parties, such as the election commission.



Fortunately, independent third parties exist to monitor the election commission.

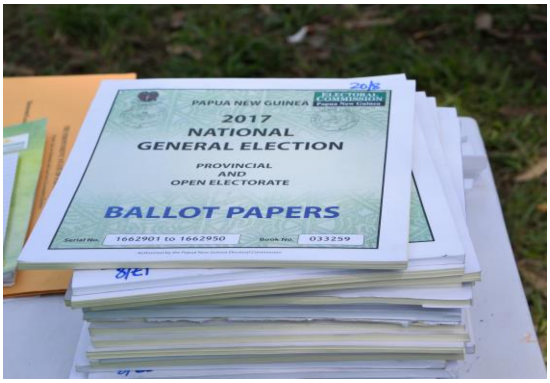
Poll Monitors
Verifying Third Parties
"Honest Keepers"

Nancy will use verifying third parties so long as they're doing their job.

It's not that verifying third parties are trustworthy. It's that Nancy can verify that the verifying third parties are indeed performing their work of verification. The verification by verifying third parties must be transparent at any point relevant to Nancy's voting.

Why are paper ballots inherently untrustworthy?

Once a paper ballot leaves a voter's hands, the voter will never be able to see it again. Paper ballots may get altered, shredded, lost, or miscounted. As a voter, you are the "first party," the person you are voting for is the "second party," and you are depending on a third party that may let you down and, most importantly, where you'll never know if they let you down.

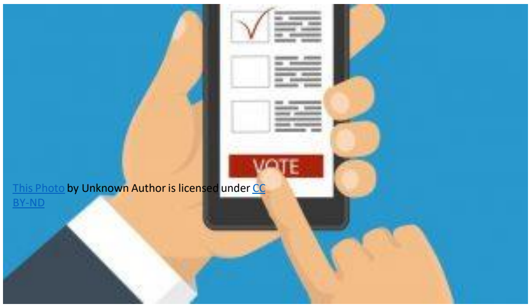


This Photo by Unknown Author is licensed under CC BY-SA-NC

How does Quintillian's advice apply to voters?

- The Roman orator Quintillian remarked: "Write not so that you will be understood but write so that you cannot be misunderstood.
- Lesson to voters: "Don't submit ballots in the hopes that they will be counted but submit ballots so bullet-proof that they CANNOT be miscounted."

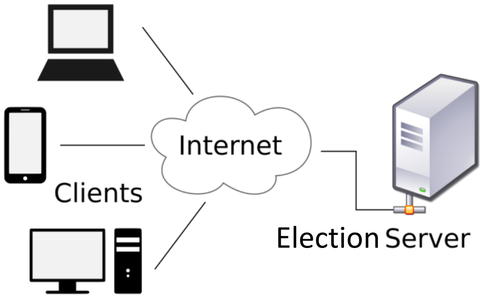
Given the right safeguards, Nancy is therefore willing to participate in a purely digital election.



With proper encryption and cybersecurity techniques, digital ballots can be made secure.

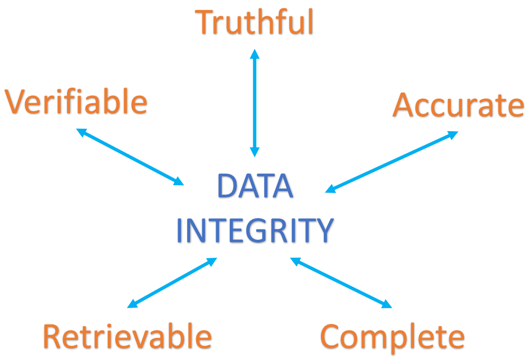
The election will be officially handled online by a server at https://alice-v-bob-election.gov.

1. A server will handle all election data at alice-v-bob-election.gov.
2. Mirror sites by "honest keepers" will provide backup for this server.
3. Data integrity methods will make sure any data on these servers is not tampered with.



What are data integrity methods?

They are methods that ensure data is not tampered with, remaining the same now as when created in the past. If the data was tampered with, such methods show definitively that the data was altered and allow for recovery of the original.



Truthful

Verifiable

Accurate

DATA INTEGRITY

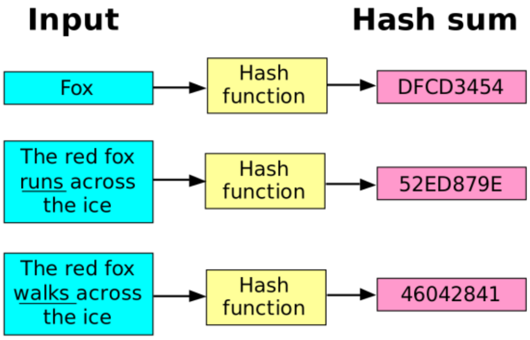
Retrievable

Complete

Two widely used data integrity techniques:

1. Hash functions.
2. Blockchains (which use multiple hash functions in series).

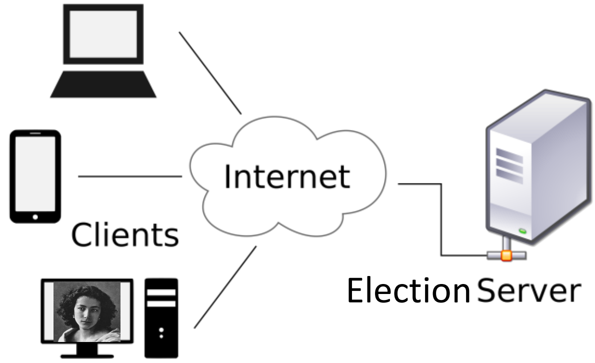
Hash functions take any text or file and give it a unique digital stamp. If the text or file is altered, the stamp changes, showing that the original was not preserved.



This Photo by Unknown Author is licensed under CC BY-SA

The first thing Nancy now needs to do is get registered to vote.

The list of registered voters is at alice-v-bob-election.gov/registered-voters.



To register to vote, Nancy does three things:

1. She submits N: her name and disambiguating information from the list of eligible voters
2. Next she submits PoI: proof of identity, which can include biometric data.
3. Finally, she creates KL1 and KL2: two cryptographic public-private keys.

Nancy's voter registration is then visible online as follows:

1. N – her name with disambiguating information is listed plainly
2. PoI – for confidentiality, her proof of identity will be encrypted as well as hashed.
3. KL1 and KL2 – two cryptographic public-private keys, with Nancy submitting for online view the public key for KL1, a hash of the private key for KL2.

Nancy’s public and private keys look as follows:

KL1:

Public key: 🔑

Private key: 🔑

KL2:

Public key: 🔑

Private key: 🔑

Nancy’s voter registration will display the following online:

1. N – her name with disambiguating information is listed plainly
2. PoI – for confidentiality, her proof of identity will be encrypted as well as hashed.
3. KL1 public key: 🔑
4. KL2 hash of private key:
   hash(🔑)

What is Nancy’s confidence that the roll of registered voters is legitimate?

Nancy knows that she is a legitimate voter and so is confident about legitimate voters like herself getting on the roll of registered voters. Also, because of rigorous PoI data collected on voters, which can be verified by third parties with sufficient access, she is confident that fraudulent voters are not easily slipping through the cracks.

The next thing Nancy will need to do is create and submit her ballot.

Nancy has decided to vote for Alice.

Alice

Nancy’s unencrypted ballot looks as follows:

OFFICIAL BALLOT

Alice ✓
Bob

100-digit cryptographic nonce:

```
45915786826944624381
27919770504579517236
59546462649671077783
26870769094406593793
23979062681624435939
```

Why does Nancy include a “cryptographic nonce” in her ballot?

By including a cryptographic nonce, in this case a 100-digit random number, Nancy makes sure her ballot, before encryption or cryptographic signing, is distinct from other ballots, thus preventing preimage attacks and possible misattributions of her ballot. In particular, the nonce allows Nancy to confirm that this is her ballot.

With the private key in KL2, Nancy cryptographically signs her ballot:

OFFICIAL BALLOT

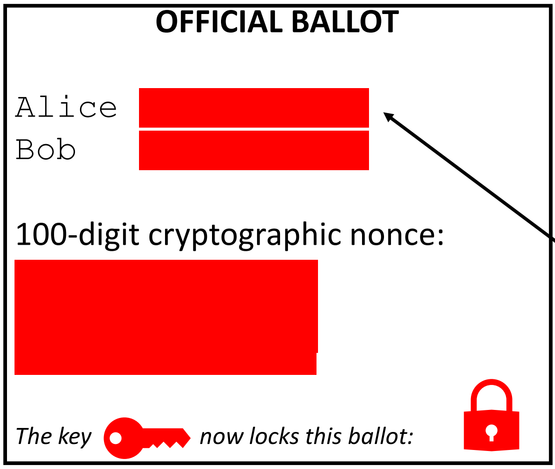
Alice [redacted]
Bob [redacted]

100-digit cryptographic nonce:

[redacted]

The key 🔑 *now locks this ballot:* 🔒

Nancy’s ballot is now cryptographically locked.


OFFICIAL BALLOT
Alice
Bob
100-digit cryptographic nonce:
The key 🔑 *now locks this ballot:* 🔒

The fact that Nancy put a check by Alice’s name is now occluded by the cryptographic lock.

Nancy next uses KL1 to upload her signed ballot at alice-v-bob-election.gov/ballots.

Specifically, Nancy inputs her public key 🔑 to identify herself and then her private key 🔑 to verify her identity, thereby authorizing her to upload her cryptographically signed ballot.

Nancy's ballot is now uploaded at alice-v-bob-election.gov/ballots.

OFFICIAL BALLOT

Alice [redacted]
Bob [redacted]

100-digit cryptographic nonce:

[redacted]

The key 🔑 *now locks this ballot:* 🔒

Because the ballot is cryptographically signed, it is unreadable.

OFFICIAL BALLOT

Alice [redacted]
Bob [redacted]

100-digit cryptographic nonce:

[redacted]

The key 🔑 *now locks this ballot:* 🔒

To preserve the secrecy of Nancy’s ballot, no tracking pixels are allowed.

OFFICIAL BALLOT

Alice

Bob

100-digit cryptographic nonce:

The key 🔑 *now locks this ballot:* 🔒

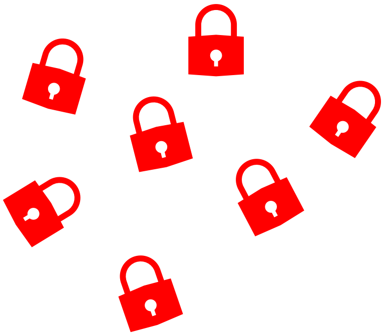
The election commission will face stiff penalities if it is discovered that they use tracking pixels to track voter identities behind ballots.

Nancy next anonymously uploads her public key from KL2 at alice-v-bob-election.gov/ballots.

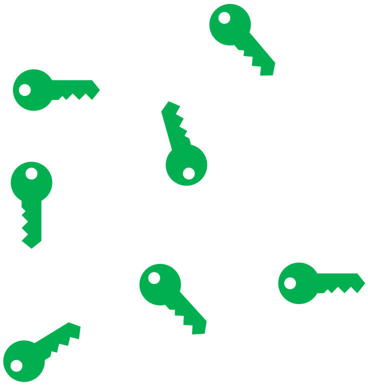
Specifically, Nancy uploads her public key 🔑 in order to unlock her ballot that was cryptographically signed with her private key 🔑 . Both the "red ballot" and the "green key" are now at alice-v-bob-election.gov/ ballots. In uploading the green key, Alice does not reveal her identity.

Encrypted ballots and decrypting keys now both exist at alice-v-bob-election.gov/ballots.

Locked (cryptographically signed) ballots:



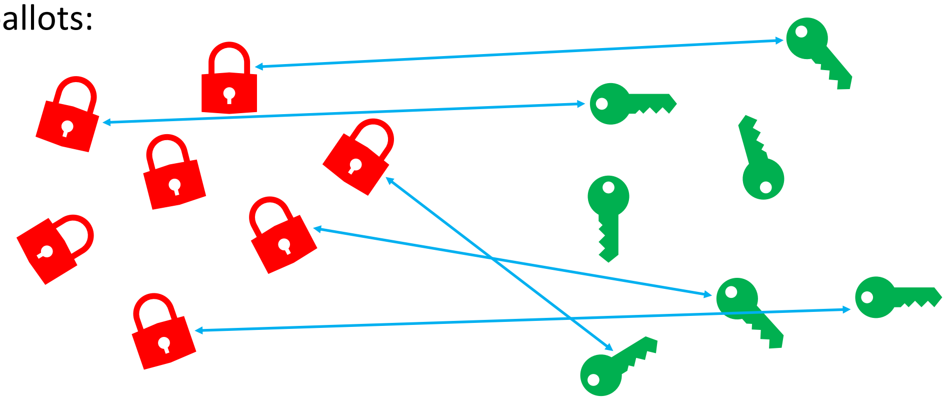
Keys that unlock ballots:



Each key can unlock at most one ballot at alice-v-bob-election.gov/ballots.

Locked (cryptographically signed) ballots:

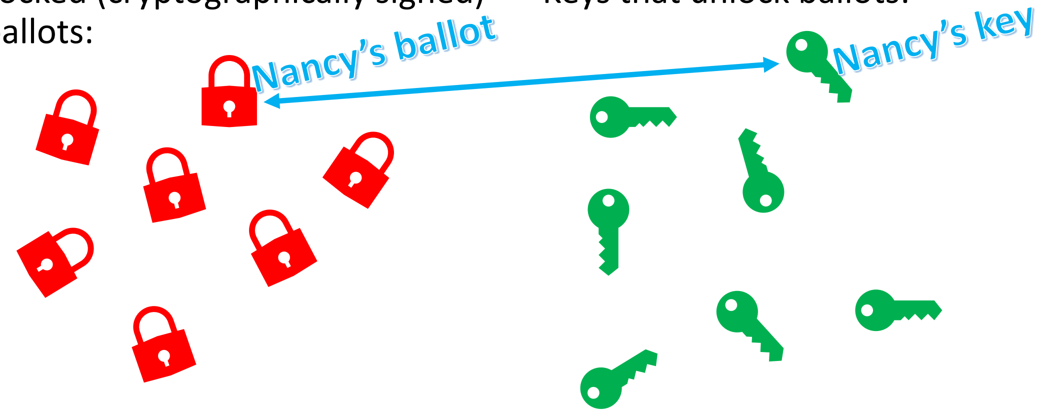
Keys that unlock ballots:



Nancy confirms that her ballot and key have both been uploaded at alice-v-bob-election.gov/ballots.

Locked (cryptographically signed) ballots:

Keys that unlock ballots:



Locks with their keys are automatically unlocked at alice-v-bob-election.gov/ballots.

The ballot that Nancy cryptographically signed and uploaded:

🔒

The public key that Nancy anonymously uploaded:

🔑

Nancy's unencrypted ballot now appears unlocked at alice-v-bob-election.gov/ballots, but without her identity:

OFFICIAL BALLOT

```
Alice ✓
Bob
```

100-digit cryptographic nonce:

```
45915786826944624381
27919770504579517236
59546462649671077783
26870769094406593793
23979062681624435939
```

[redacted]

The vote is for Alice:

OFFICIAL BALLOT

```
Alice ✓
Bob
```

100-digit cryptographic nonce:

```
45915786826944624381
27919770504579517236
59546462649671077783
26870769094406593793
23979062681624435939
```

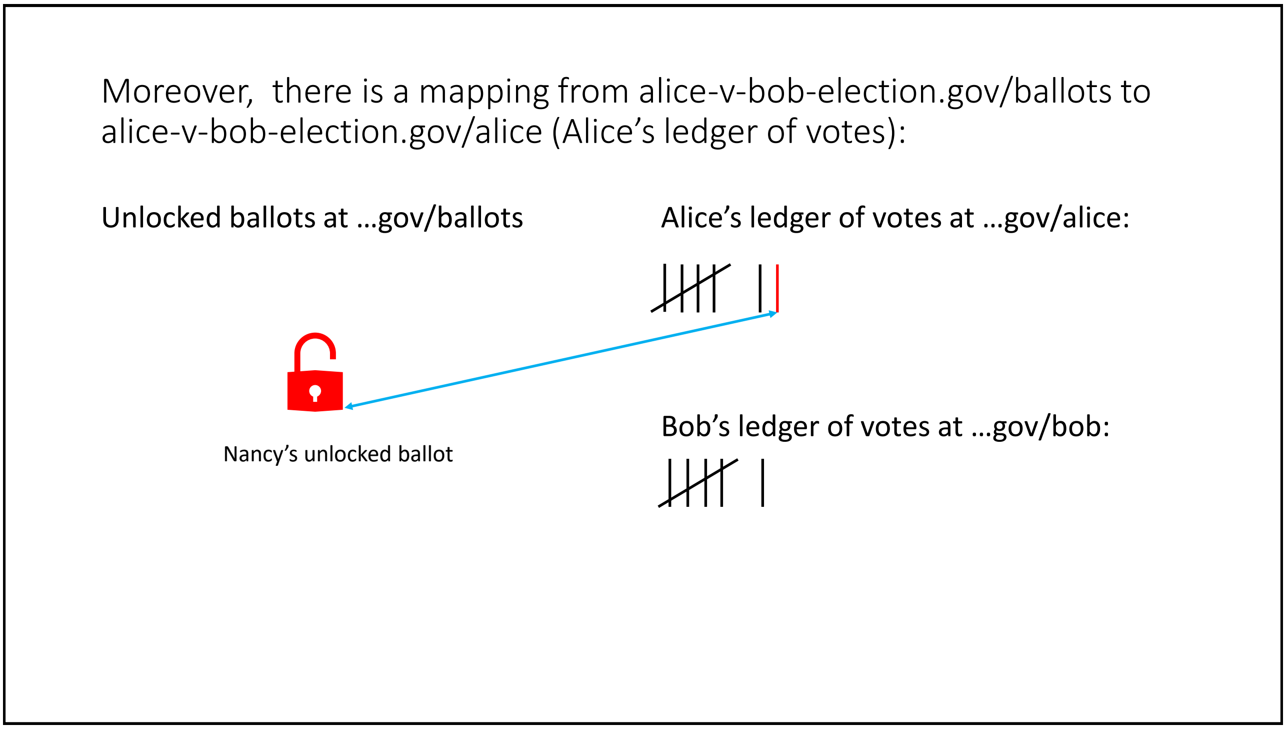
That vote now is credited to Alice.

OFFICIAL BALLOT

```
Alice ✓
Bob
```

100-digit cryptographic nonce:

```
45915786826944624381
27919770504579517236
59546462649671077783
26870769094406593793
23979062681624435939
```



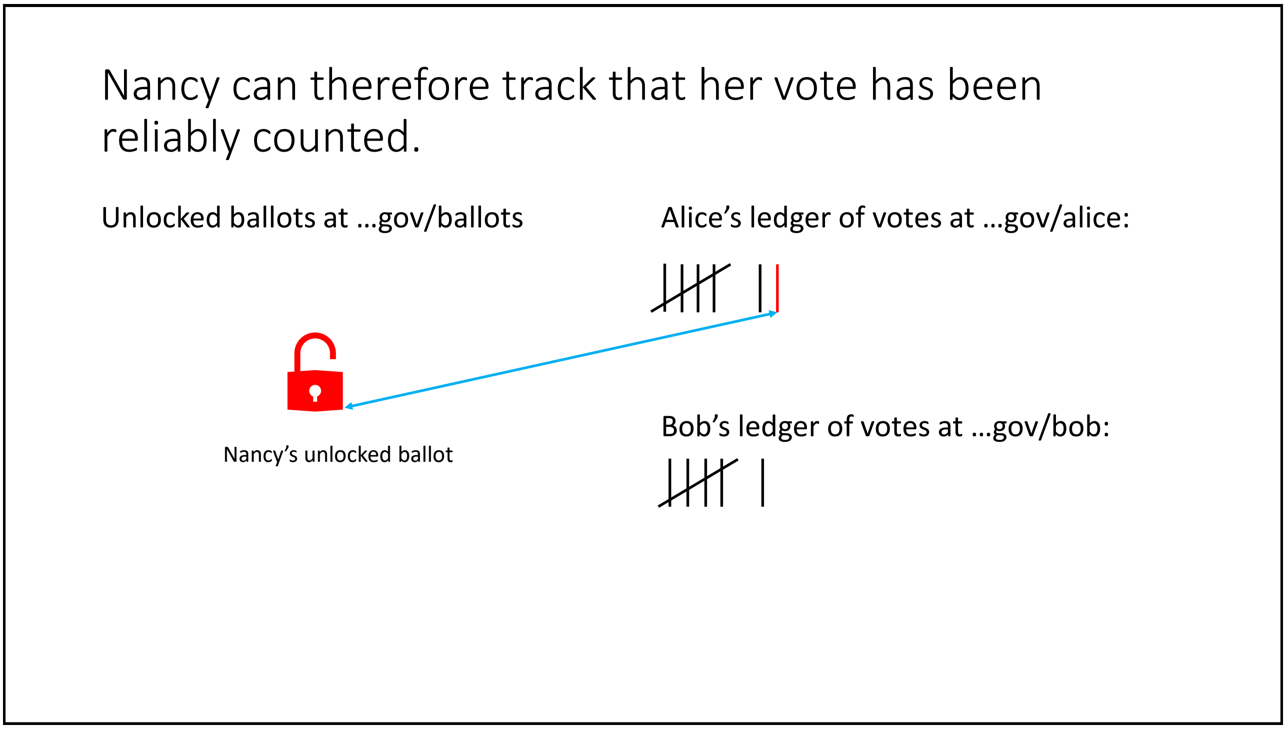
Moreover, there is a mapping from alice-v-bob-election.gov/ballots to alice-v-bob-election.gov/alice (Alice’s ledger of votes):

Unlocked ballots at …gov/ballots

Alice’s ledger of votes at …gov/alice:

Nancy’s unlocked ballot

Bob’s ledger of votes at …gov/bob:



Nancy can therefore track that her vote has been reliably counted.

Unlocked ballots at …gov/ballots

Alice’s ledger of votes at …gov/alice:

Nancy’s unlocked ballot

Bob’s ledger of votes at …gov/bob:

The details of the Cryptosecure Election Protocol (CEP) can be found at Expensivity.com:

https://expensivity.com/financial-v-election-fraud-and-security/

All images are taken from Wikimedia and Creative Commons.