Secure Election System with Blockchain

Blockchain enabled E-voting

Esref Ozturk
esref.ozturk@ceng.metu.edu.tr

Wireless Systems, Networks and Cybersecurity Laboratory
Department of Computer Engineering
Middle East Technical University
Ankara Turkey

October 16, 2018

Outline of the Presentation

Election Cheating

Requirements	Traditional
Verifiability	P
Anonimity	P
Accuracy	P
Transparency	P
Consistency	P

- Y : Yes
- N : No
- P : Partial

Blockchain Integration

- What is Blockchain?
- Blockchain Usage in Elections to Store Votes

Motivation/Importance

Requirements	Traditional	Blockchain
Verifiability	P	Y
Anonimity	P	Y
Accuracy	P	Y
Transparency	P	Y
Consistency	P	Y

- Y : Yes
- N : No
- P : Partial

Background

Requirements	Traditional	Blockchain	E-Voting	Early Blockchain
Verifiability	P	Y	P	Y
Anonimity	P	Y	N	Y
Accuracy	P	Y	N	P
Transparency	P	Y	N	P
Consistency	P	Y	P	Y

- Y : Yes
- N : No
- P : Partial

Main Idea

- Blockchain
- Blind Signature
- Encryption
- Inspectors

Before Election

1. A generates two public-key/private-key pairs: a,b and c,d
   - a,b will be used for signing
   - c,d will be used for encryption
2. A broadcasts a and c
3. I generates two public-key/private-key pairs: e,f and g,h
   - e,f will be used for signing
   - g,h will be used for encryption
4. I broadcasts e and g

During Election

1. V chooses a vote: v
2. V chooses a random string: r
3. V sends $B(E_I(E_A(v, r)))$ to A
4. A sends $S_A(B(E_I(E_A(v, r))))$ to V
5. V sends $B(S_A(E_I(E_A(v, r))))$ to I
6. I sends $S_I(B(S_A(E_I(E_A(v, r)))))$ to V
7. V sends $S_I(S_A(E_I(E_A(v, r)))), E_I(E_A(v, r))$ to B
   - At this step anyone can check the sign of the message

After Election

1. A broadcasts d, I broadcasts h
   - After this step, everyone instantly will know the results since they can decrypt all the votes

Conclusions

Requirements	Traditional	Blockchain	E-Voting	Early Blockchain
Verifiability	P	Y	P	Y
Anonimity	P	Y	N	Y
Accuracy	P	Y	N	P
Transparency	P	Y	N	P
Consistency	P	Y	P	Y

- Y : Yes
- N : No
- P : Partial

Questions

THANK YOU

Secure Election System with Blockchain
Blockchain enabled E-voting

presented by Esref Ozturk
esref.ozturk@ceng.metu.edu.tr

October 16, 2018