E-vote with Blockchain and Municipal referenda

The case of a bottom-up proposal in Naples

Mauro Forte

Municipality of Napoli

Diego Romano

Institute for High Performance Computing and Networking

of the Italian National Research Council (ICAR-CNR)

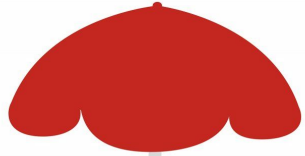DecidimFest 2019, 29 Oct - 31 Oct Fabra i Coats (Barcelona)

is
this
still
the way?

some great experiments... but problems...

democracy needs a new way
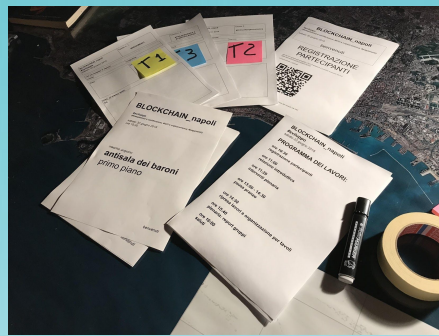
E-voting?

1) Electronic voting on the Internet

2) Electronic voting in the polling station

E-voting?

1) Electronic voting on the Internet

2) Electronic voting in the polling station

Unsuitable when TRUE anonymity is at risk
- Authentication procedure to authorize the single vote
- Traceability of data packages
  (remediable with sophisticated protocols like TOR)

Facilitates coercion and vote trading:
- Voting could be non-private

What about Blockchain?

Blockchain e-vote on the Internet?
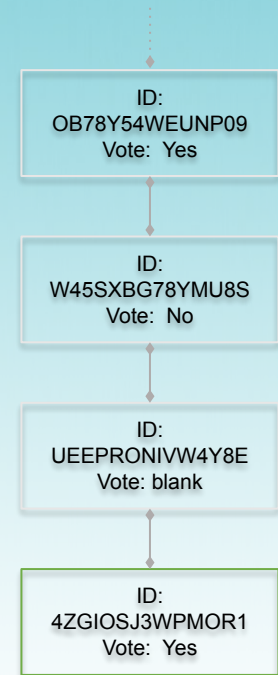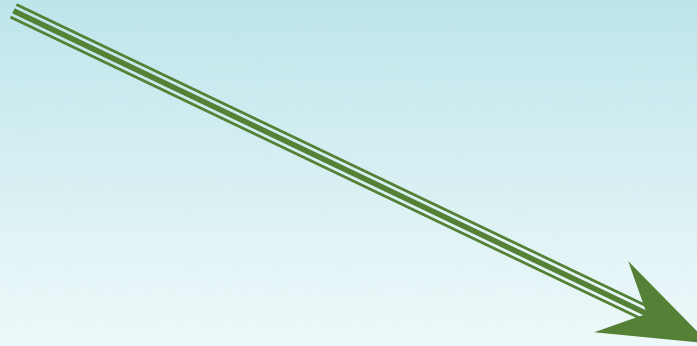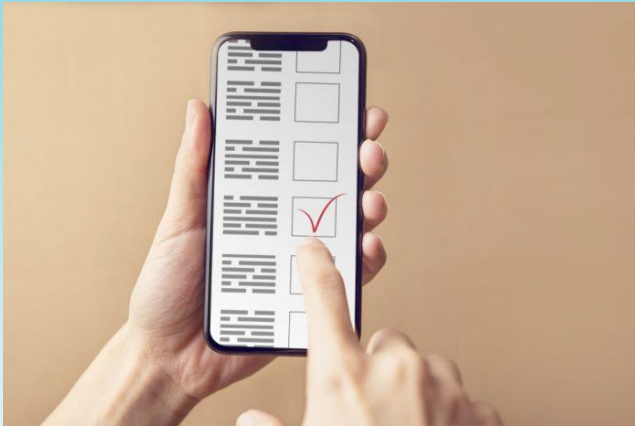
Blockchain e-vote on the Internet?

Some problems!

ID: OB78Y54WEUNP09
Vote: Yes

ID: W45SXBG78YMU8S
Vote: No

ID: UEEPRONIVW4Y8E
Vote: blank

ID: 4ZGIOSJ3WPMOR1
Vote: Yes

Blockchain e-vote on the Internet?

ID:
OB78Y54WEUNP09
Vote: Yes

ID:
W45SXBG78YMU8S
Vote: No

ID:
UEEPRONIVW4Y8E
Vote: blank

ID:
4ZGIOSJ3WPMOR1
Vote: Yes
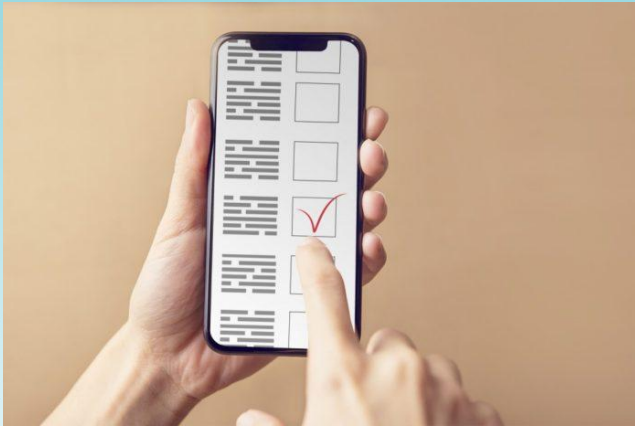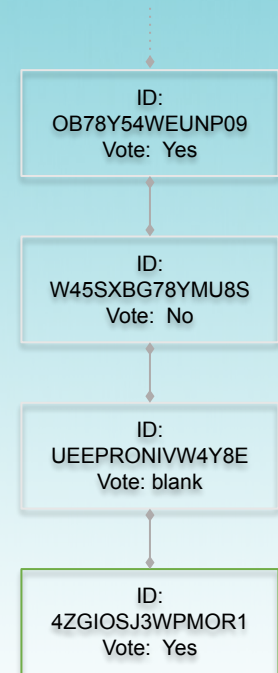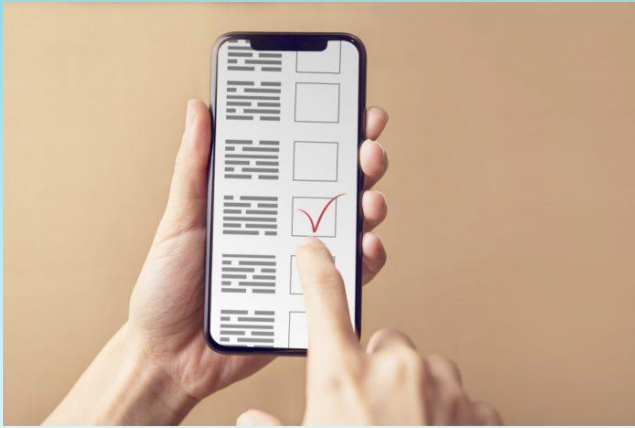
Some problems!

- Anonymity?

Blockchain e-vote on the Internet?

ID:
OB78Y54WEUNP09
Vote: Yes

ID:
W45SXBG78YMU8S
Vote: No

ID:
UEEPRONIVW4Y8E
Vote: blank

ID:
4ZGIOSJ3WPMOR1
Vote: Yes
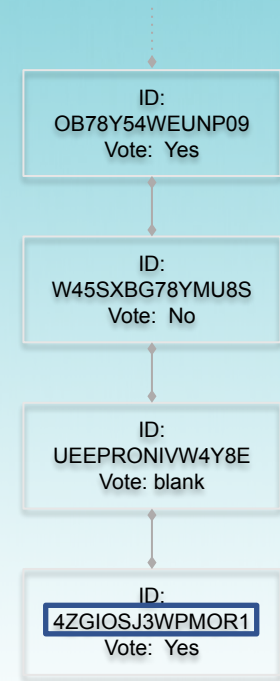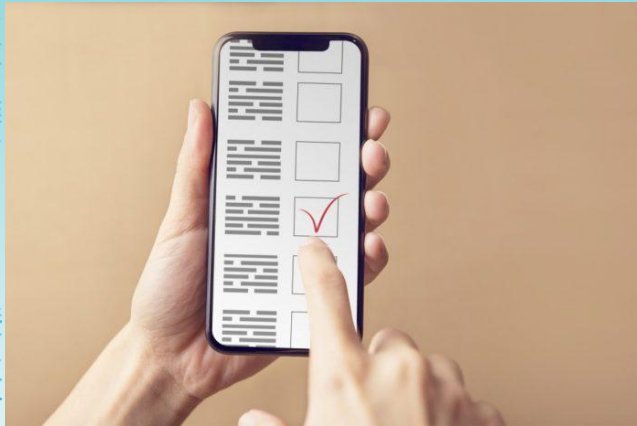
Some problems!

- Open ballot box results!
- Anonymity?

Blockchain e-vote on the Internet?

Some problems!

ID:
OB78Y54WEUNP09
Vote: Yes

ID:
W45SXBG78YMU8S
Vote: No

ID:
UEEPRONIVW4Y8E
Vote: blank

ID:
4ZGIOSJ3WPMOR1
Vote: Yes

- Who is really voting?
- Open ballot box results!
- Anonymity?

Some solutions

ID:
OB78Y54WEUNP09
Vote: Yes

ID:
W45SXBG78YMU8S
Vote: No

ID:
UEEPRONIVW4Y8E
Vote: blank

ID:
4ZGIOSJ3WPMOR1
Vote: Yes

- Who is really voting?
- Open ballot box results!
- Anonymity?

Some solutions

- ## Who is really voting?
- Open ballot box results!
- Anonymity?

- ## VOTE IN THE POLLING STATION

➔ Voter identity check
➔ Use of a preconfigured device
➔ *Open Source Software*

ID:
OB78Y54WEUNP09
Vote: Yes

ID:
W45SXBG78YMU8S
Vote: No

ID:
UEEPRONIVW4Y8E
Vote: blank

ID:
4ZGIOSJ3WPMOR1
Vote: Yes

Some solutions

- Who is really voting?
- Open ballot box results!
- Anonymity?

- VOTE IN THE POLLING STATION

→ Voter identity check
→ Use of a preconfigured device
→ *Open Source Software*

- VOTE ENCRYPTION

| ID: OB78Y54WEUNP09 |
| Voto: xjhgejì |

| ID: W45SXBG78YMU8S |
| Voto: ijgfjsd |

| ID: UEEPRONIVW4Y8E |
| Voto: uehckjh |

| ID: 4ZGIOSJ3WPMOR1 |
| Voto: tuhgjhd |

Some solutions

- Who is really voting?
- Open ballot box results!
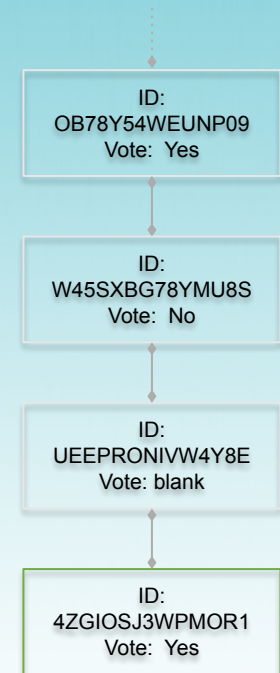
- Anonymity?

- VOTE IN THE POLLING STATION

→ Voter identity check
→ Use of a preconfigured device
→ *Open Source Software*

- VOTE ENCRYPTION

- VIRTUAL BALLOT BOX

→ Votes are aggregated

ID polling station:
OB78Y54WEUNP09
Votes:
xjhgejì
kfjdlsk
asdoih
grjiwo

ID polling station:
4ZGIOSJ3WPMOR1
Votes:
tuhgjhd
sdakljòl
dfskjlkjk
aidsaoijs
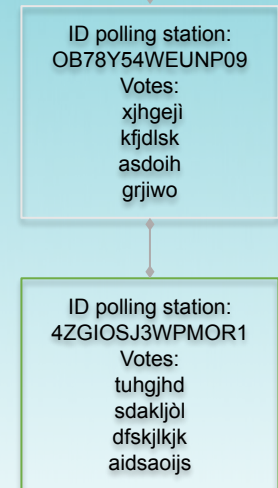
E-voting?

1) ~~Electronic voting on the Internet~~

2) Electronic voting in the polling station

- Polling stations and places do not change much
- Costs for appliance and personnel do change
- New benefits
- New risks

Current setting

Polling station
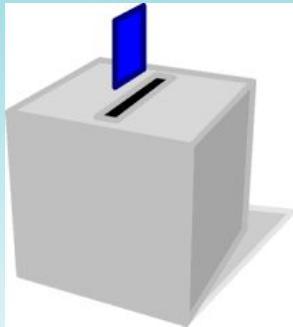
Set up of polling station
Voters identification
Authorization (giving ballot paper)
Vote expression (in voting booth)
Collection
Counting votes
Delivery of parcels

Municipal Electoral Office

Managing of electoral rolls
Managing right of voting certificates
Division of municipality wrt polling stations
Support of polling officers and staff
Managing of the count staff list
Managing of the polling officers list
Organization of consultations
Issuing of electoral certificates

Setting for blockchain e-vote

Polling station

Set up of polling station
Voters identification
Authorization (giving ballot paper)
Vote expression (in voting booth)
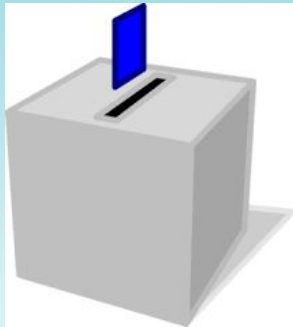Collection
Counting votes
Delivery of parcels

Changed

Municipal Electoral Office

Managing of electoral rolls
Managing right of voting certificates
Division of municipality wrt polling stations
Support of polling officers and staff
Managing of the count staff list
Managing of the polling officers list
Organization of consultations
Issuing of electoral certificates

Unchanged

Polling Station n. 5

OK

Polling Station

n. 5

REFERENDUM - MUNICIPAL CONSULTATION

What is your answer to the question which interests the local community?

YES   blank   null
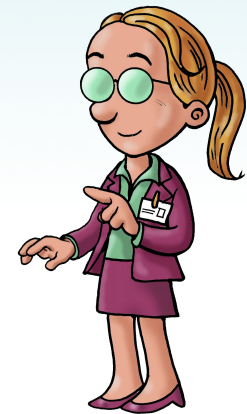
Polling
Station
n. 5

Polling
Station
n. 1

Polling
Station
n. 2

Polling
Station
n. 5

Polling
Station
n. 1

Polling
Station
n. 2

Polling
Station
n. 5

Polling
Station
n. 1

Polling
Station
n. 2

ID polling station:
OB78Y54WEUNP09
Votes:
xjhgejì
kfjdlsk
asdoih
grjiwo

ID polling station:
4ZGIOSJ3WPMOR1
Votes:
tuhgjhd
sdakljòl
dfskjlkjk
aidsaoijs

ID polling station:
OB78Y54WEUNP09
Votes:
xjhgeji
kfjdlsk
asdoih
grjiwo

ID polling station:
4ZGIOSJ3WPMOR1
Votes:
tuhgjhd
sdakljòl
dfskjlkjk
aidsaoijs

ID polling station:
4ZGIOSJ3WPMOR1
Key:
6S3js6hAC686K2bm1

STOP
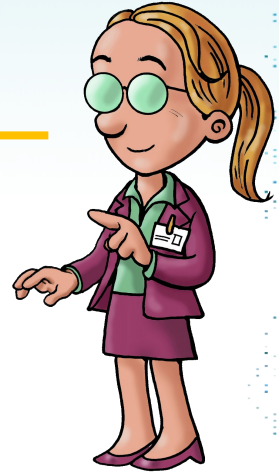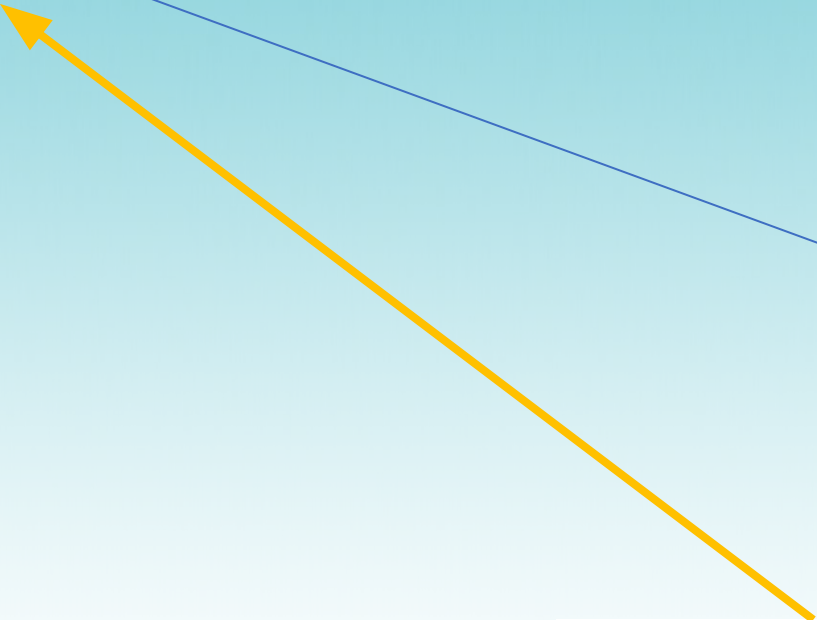
YES   NO   blank   null
123   375   8   13

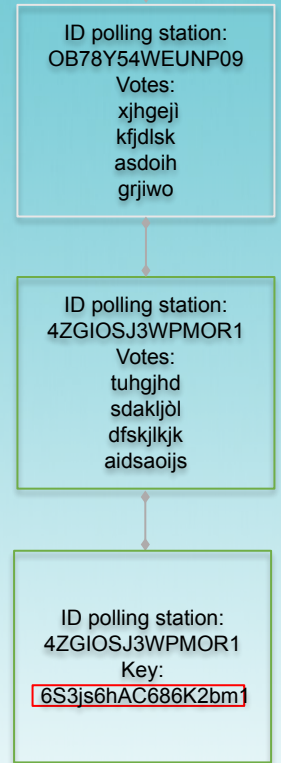ID polling station:
OB78Y54WEUNP09
Votes:
xjhgeji
kfjdlsk
asdoih
grjiwo

ID polling station:
4ZGIOSJ3WPMOR1
Votes:
tuhgjhd
sdakljòl
dfskjlkjk
aidsaoijs

ID polling station:
4ZGIOSJ3WPMOR1
Key:
6S3js6hAC686K2bm1

More opportunities

To limit vote trading

- The interface provides the possibility to change the vote before leaving the booth
- The use of the smartphone camera loses its value
- The vote is placed in the ballot box ONLY when the identity document is returned

REFERENDUM - MUNICIPAL CONSULTATION

What is your answer to the question which interests the local community?

YES   NO   blank   null

Do you want to change your vote?

ADVANTAGES

- Reducing paperwork and therefore sources of error

- Keeping a consolidated procedure as much as possible

- Making hourly turnout statistics possible

- Making mistakes in counting votes almost zero

- Hindering the vote trading

AND…

- The publication of partial results remains impossible

- The anonymity of the voter is guaranteed

Risks and mitigation

- Network attack to system and to SW –> security by design

- Network fault –> encrypted local record of partial results until the transaction is confirmed

- Decryption of partial results –> implementation of standard key confidentiality procedures

- Anonymity of the voter –> grouping of votes in blocks of N elements

FACILITATION FROM THE DISTRIBUTED SYSTEM

Open Points

- Trust in the supply chain
  (we can be inspired by ATM solutions)

- Public verifiability:
  - Open Source code
  - Dynamic certification of the code in execution
  - Verifiability of the vote VS. anonymity

thank you!

e-voting voluntary group in napoli is:

- **Tommaso Coppola**
- **Maria Francesca De Tullio**
- **Mauro Forte**
- **Davide Lo Pilato**
- **Diego Romano**
- **Rosario Scognamiglio**
- **Erica Vaccaro**

mauro.forte@comune.napoli.it
diego.romano@cnr.it