

Blockchain-based Remote Electronic Voting

**Christian Killer, Bruno Rodrigues, Eder Scheid, Muriel Franco,
Prof. Dr. Burkhard Stiller**

*Communication Systems Group CSG,
Department of Informatics IfI, University of Zürich UZH
[killer,rodrigues,scheid,franco,stiller]@ifi.uzh.ch*



**Universität
Zürich^{UZH}**

*With many thanks addressed to M. Eck,
A. Scheitlin, N. Zaugg, R. Matile, and all @ CSG*



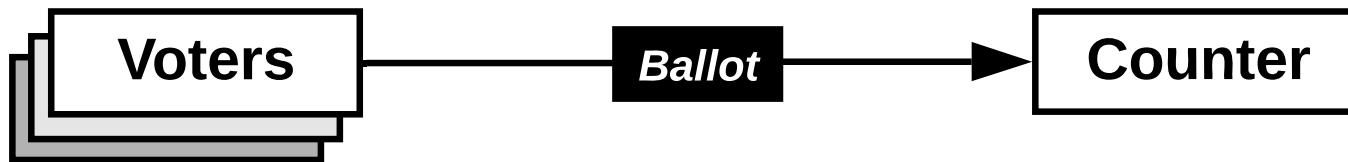
ToC

- **Electronic Voting (EV)**
 - Definitions and Notions with a Global Overview on EV
 - History of Switzerland and REV
 - Focus on Remote Postal Voting (RPV) in Switzerland
- **Remote Electronic Voting (REV)**
 - REV Requirements and Properties
 - Building Blocks
 - Homomorphic Encryption, ZKP, PBB
- **BC-based REV**
 - Provotum Voting Protocol and Evaluation
- **Summary**

Electronic Voting (EV)

- **Definitions and Notions with a Global Overview on EV**
- History of Switzerland and REV
- Focus on Remote Postal Voting (RPV) in Switzerland

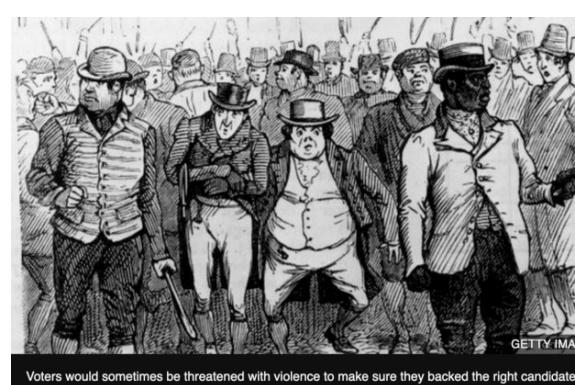
Are elections just counting?



- Main difficulties in practice
 - No one is trusted
 - Anyone is a potential adversary
 - The need for evidence
 - Any observer should be able to verify the election data
 - The secret ballot
 - Voters should not be able to prove how they voted to anyone, even if they wish to do so

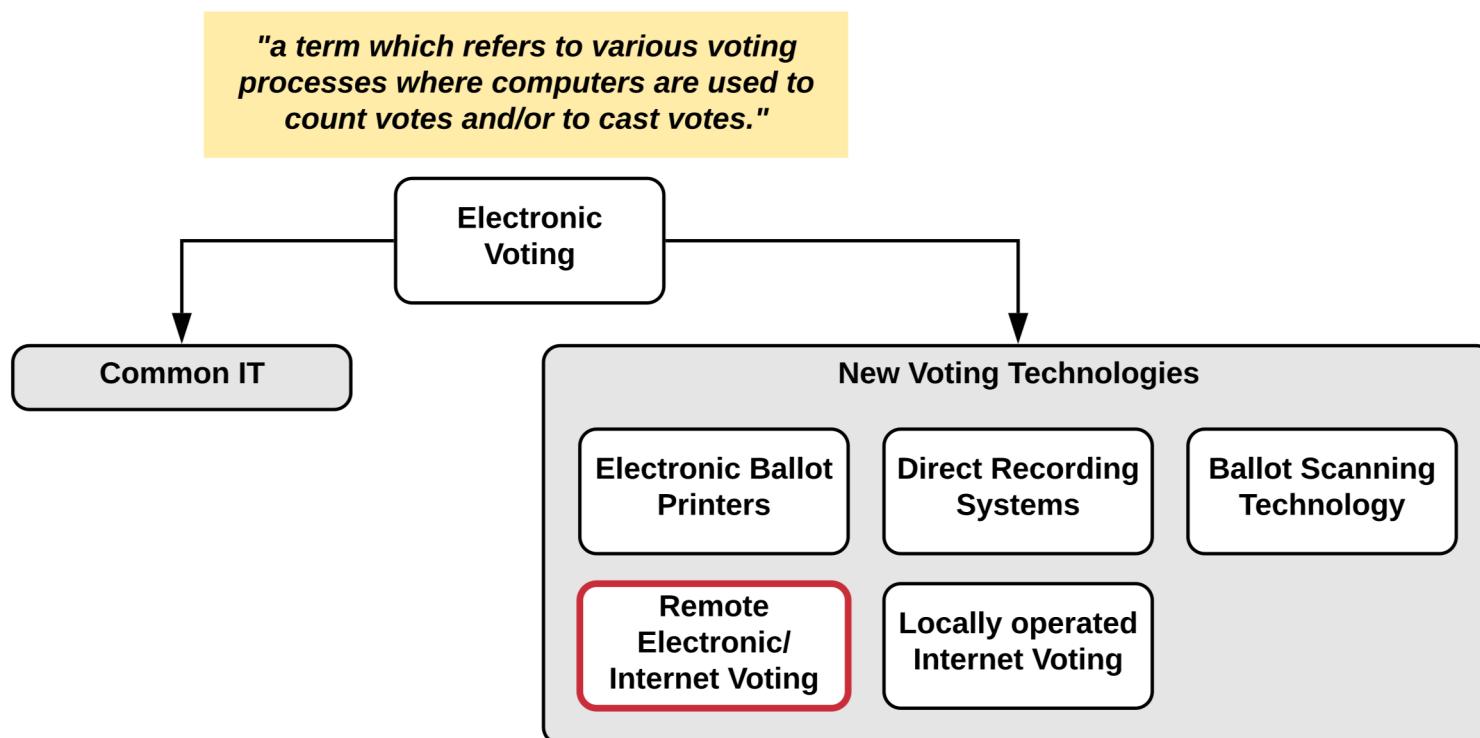
The Secret Ballot

- Mid 19th century, the “Australian ballot” was introduced as a means of deterring coercion
- Today, society takes for granted this process of voting privately within a public environment, where observers can enforce privacy, but great innovation in its time
- In the early 1980s, cryptographers began to propose new election designs with new properties and integrity guarantees

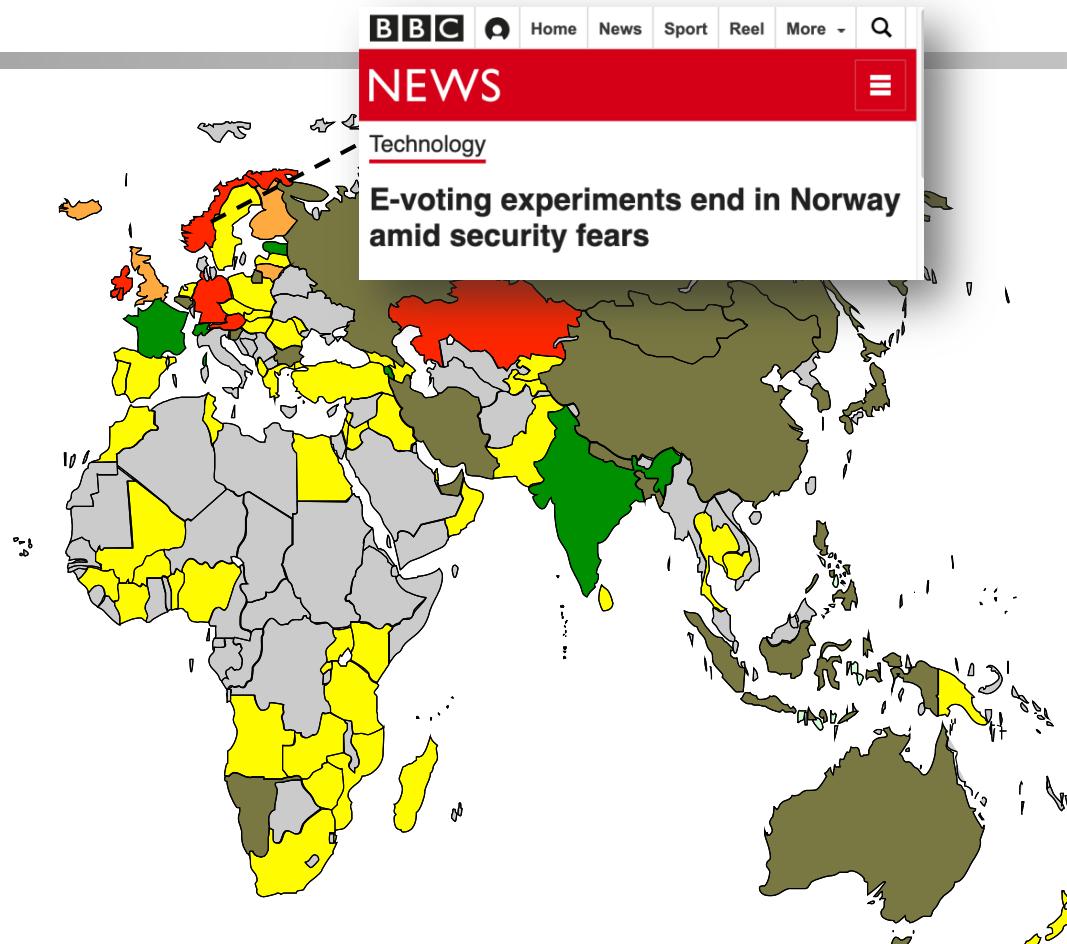


Terminology

- **Remote Electronic Voting (REV) or Internet Voting**
 - Vote cast in a **remote, uncontrolled** environment and **not** in a voting booth.



E-Voting World Map



- No plans
- Stopped use of voting technologies
- Discussion with concrete plans for Internet voting
- Discussion and/or voting technology pilots
- Internet voting (legally binding) with other voting technologies
- Ballot scanners and/or Electronic Voting Machines (legally binding)

Estonia

i-Voting saves over
11,000
working days per election

44%
of Estonians use i-Voting
844
years of working time saved

From
2005
Estonia uses i-Voting

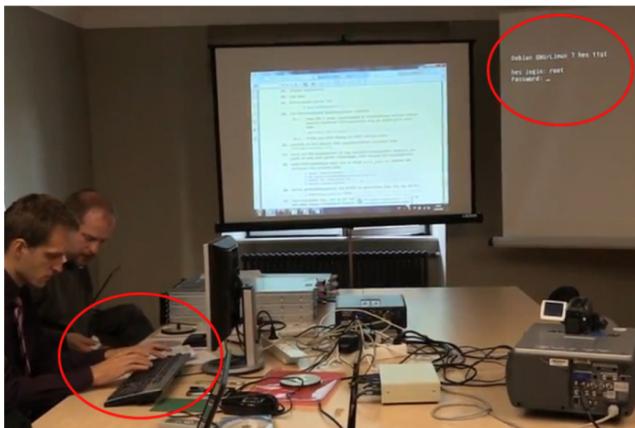


Figure 7: **Keystrokes reveal root passwords** — Videos posted by officials during the election show operators typing, inadvertently revealing root passwords for election servers.



Figure 8: **Video shows national ID PINs** — During pre-election setup, someone types the secret PINs for their national ID card in full view of the official video camera.

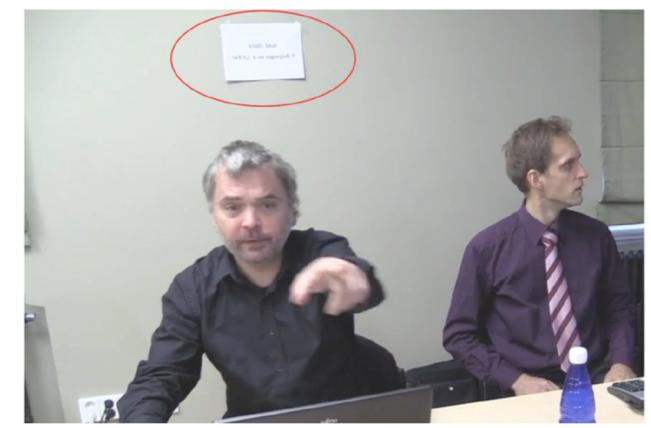


Figure 9: **Posted Wi-Fi credentials** — The official video of the pre-election process reveals credentials for the election officials' Wi-Fi network, which are posted on the wall.

Electronic Voting (EV)

- Definitions and Notions with a Global Overview on EV
- **History of Switzerland and REV**
- Focus on Remote Postal Voting (RPV) in Switzerland

Brief History of Swiss Voting Channels

- A tradition of direct democracy (Landsgemeinde)
 - Introduction of “Remote Postal Voting” in the 1970’s which was generalized in the 1990’s
 - 1998: the Federal Council proposes to study Internet Voting (I-Voting) and by the year 2000, official start of the Vote “électronique” project with three pilot cantons (GE, NE, ZH)



Image: Samuel Trümpy Photography, <https://www.gl.ch/landsgemeinde.html/216>

Current Situation in Switzerland



COUNCIL OF THE SWISS ABROAD Expat Swiss push for e-voting despite reluctance at home

The expat Swiss assembly has given the green light for an online petition calling for the introduction of e-voting by 2021.

By Urs Geiser in Visp



UNIVERSAL VERIFIABILITY Hackers uncover 'significant' flaw in Swiss Post e-voting

Hackers reported a major bug in the new Swiss Post's e-voting system as part of a public intrusion test. Swiss Post has resolved the issue.

Mar 12, 2019 - 14:03



ONLINE DEMOCRACY Opposition against e-voting project gathers pace

A committee of politicians and IT experts launches an initiative aimed at banning online voting for at least five years in Switzerland.

Electronic Voting (EV)

- Definitions and Notions with a Global Overview on EV
- History of Switzerland and REV
- Focus on Remote Postal Voting (RPV) in Switzerland**

Comparing “Systems”

RPV ? REV

REMOTE
POSTAL
VOTING

MORE
SECURE
THAN

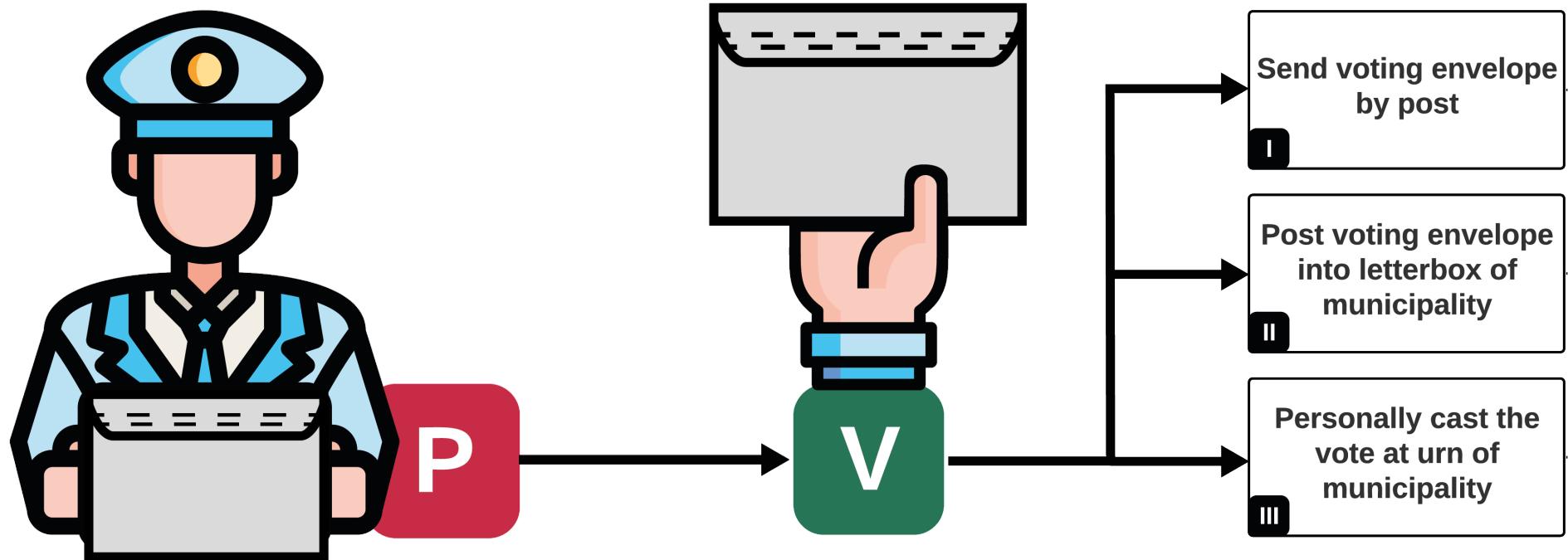
REMOTE
ELECTRONIC
VOTING

?

The Swiss RPV Case

- The Swiss RPV is **fragmented and difficult to generalize**, due to federalism in Switzerland, autonomy, and involvement of many external suppliers
- **Goal:**
To identify weaknesses of RPV to allow for “hardening” of the RPV through security and risk assessment.
 - **Disclaimer:** Focus on generalization, may not cover all cantons and processes exactly, leaves room for exceptions.
 - Many exchanges with Swiss authorities and external suppliers

RPV From a Voter's Perspective

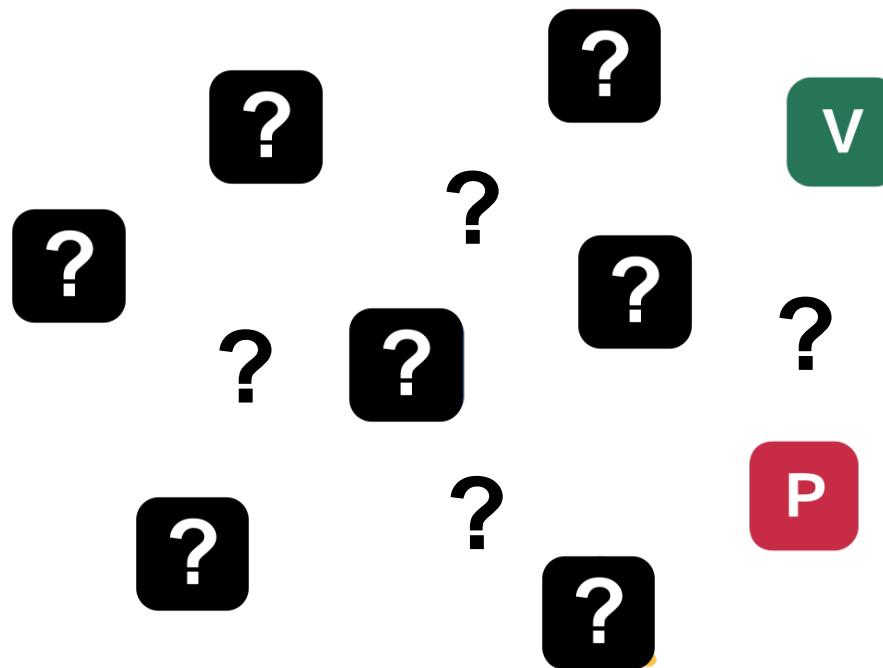


RPV: Remote Postal Voting

PVPF: Postal Voting Process Flow



Identification of Stakeholders

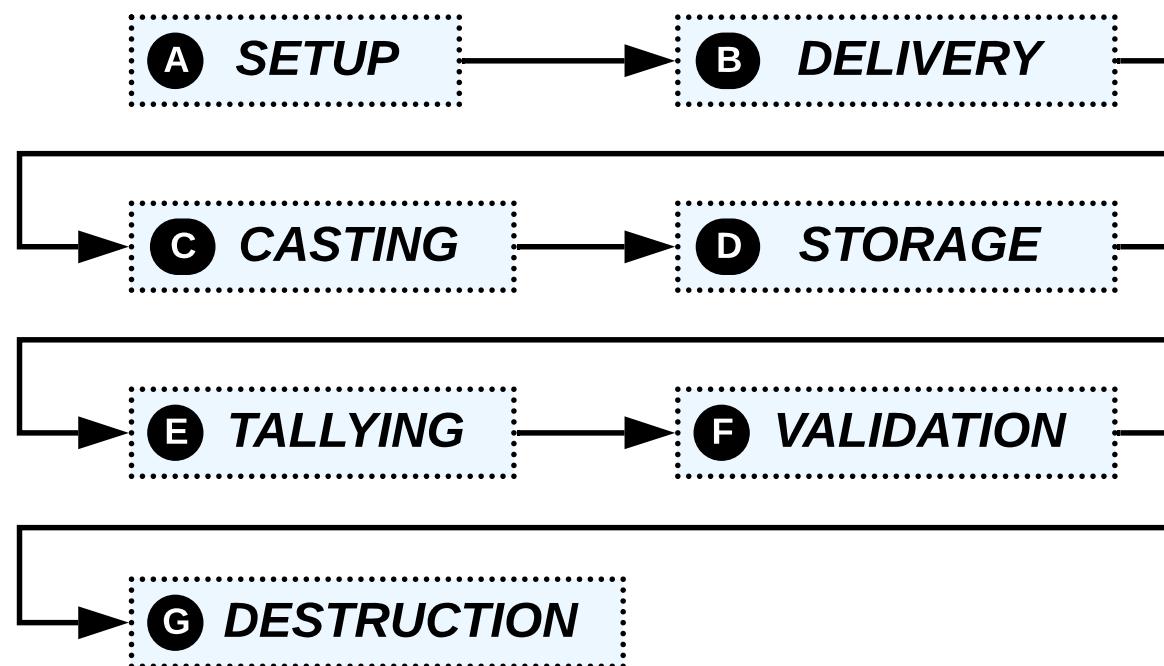


- ? Federal Government
 - ? Federal Chancellery
 - ? Cantonal Government
 - ? Municipality
 - ? Municipal Election Office
 - ? Eligible Voter
 - ? The Swiss Post
 - ? External Supplier
 - ? Security Threat

PVPF Phases

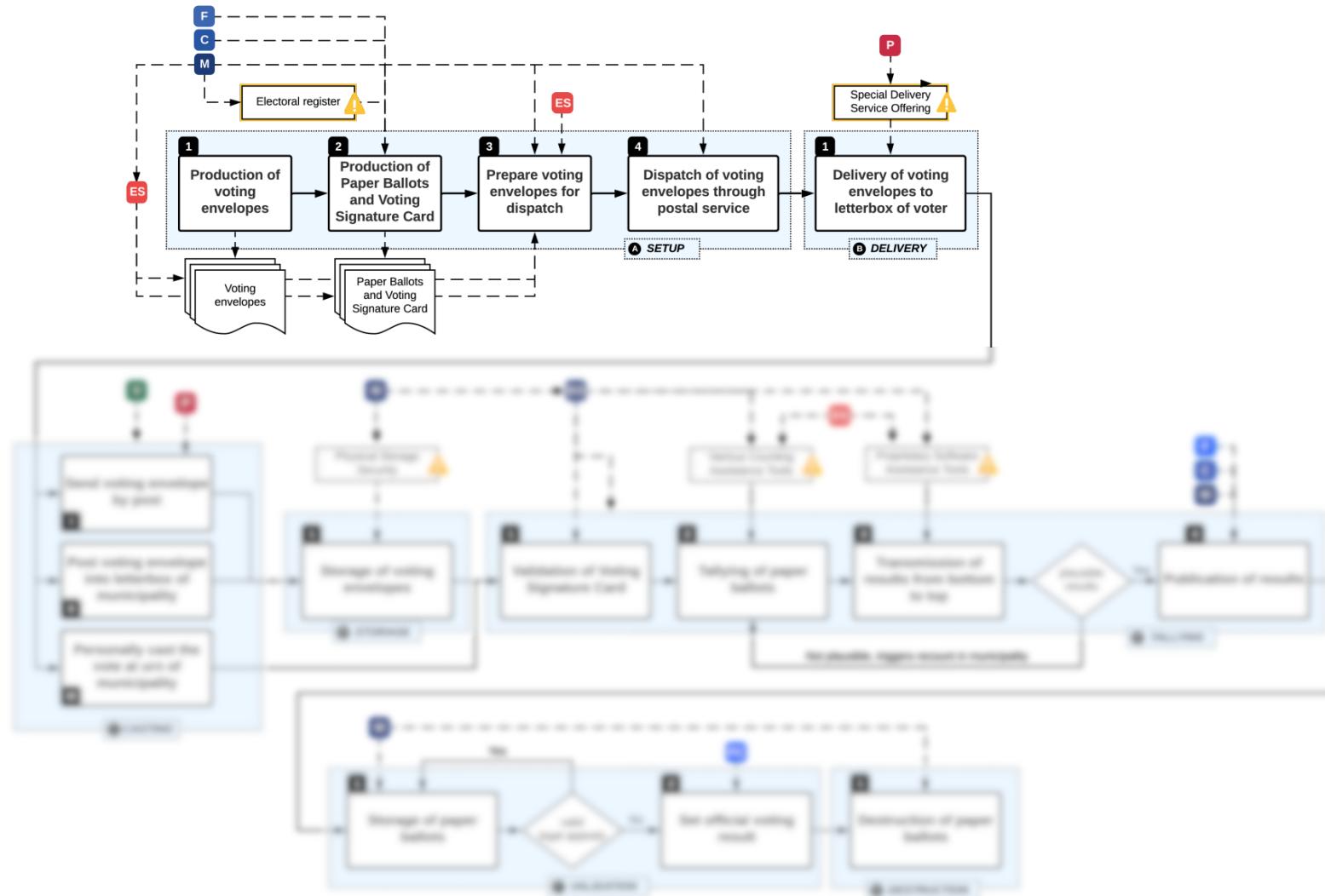
- Divided into phases A to G with various stakeholders

F	Federal Government
FC	Federal Chancellery
C	Cantonal Government
M	Municipality
EO	Municipal Election Office
V	Eligible Voter
P	The Swiss Post
ES	External Supplier
⚠	Security Threat



PVPF: Postal Voting Process Flow

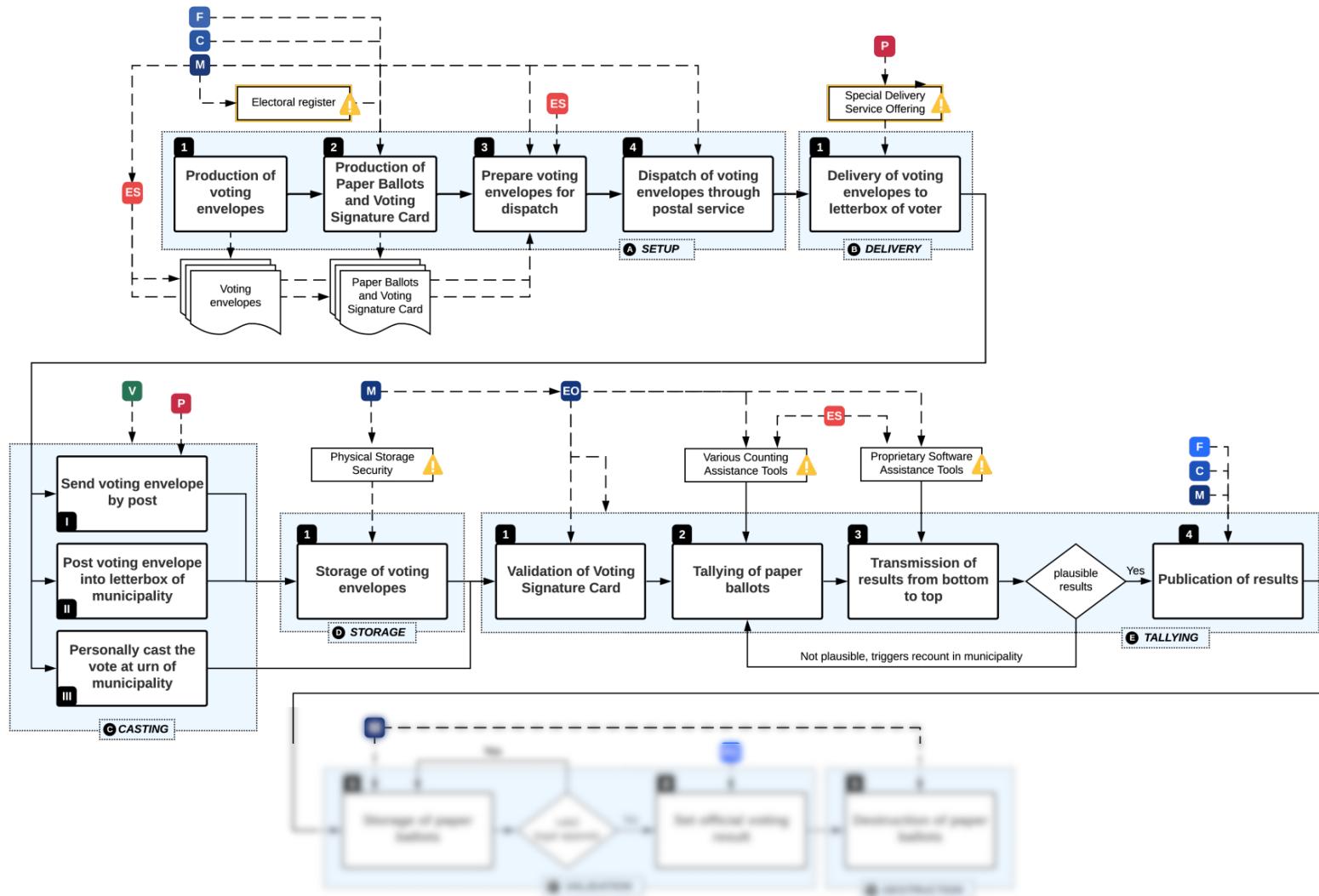
PVPF in Detail (1)



[KS19]

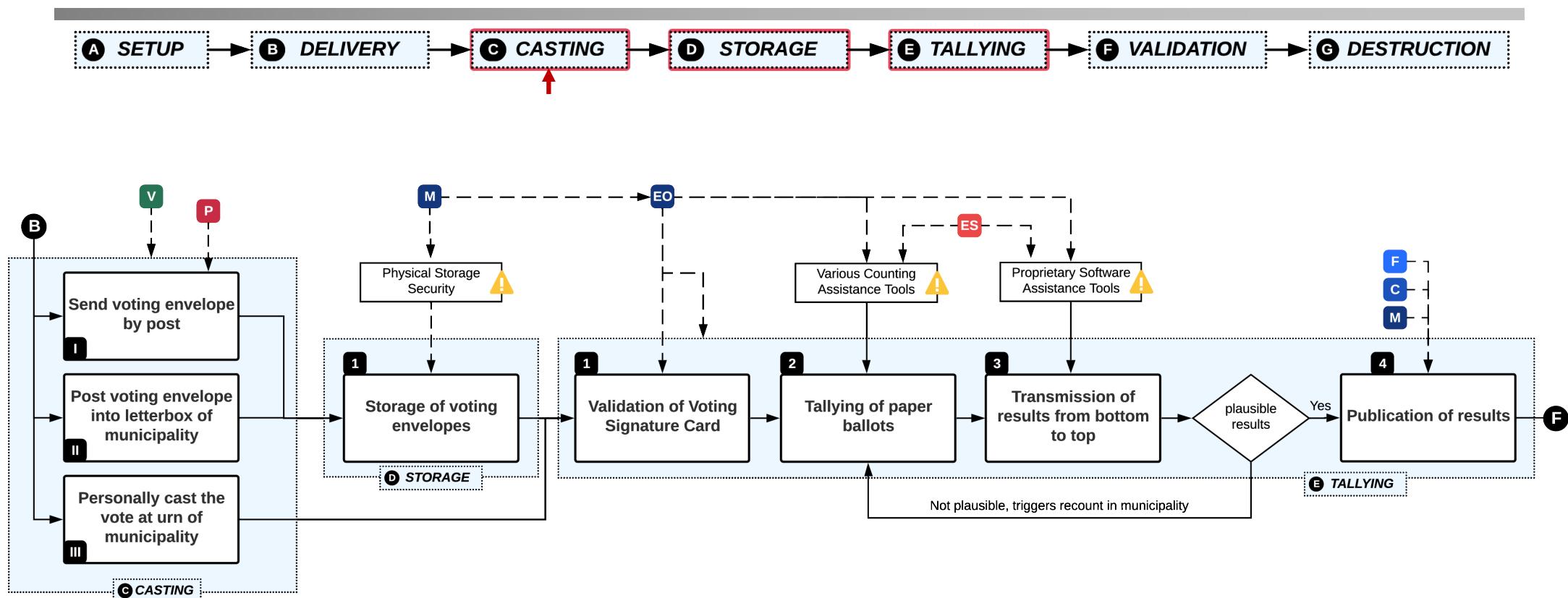
PVPF: Postal Voting Process Flow

PVPF in Detail (2)



PVPF: Postal Voting Process Flow

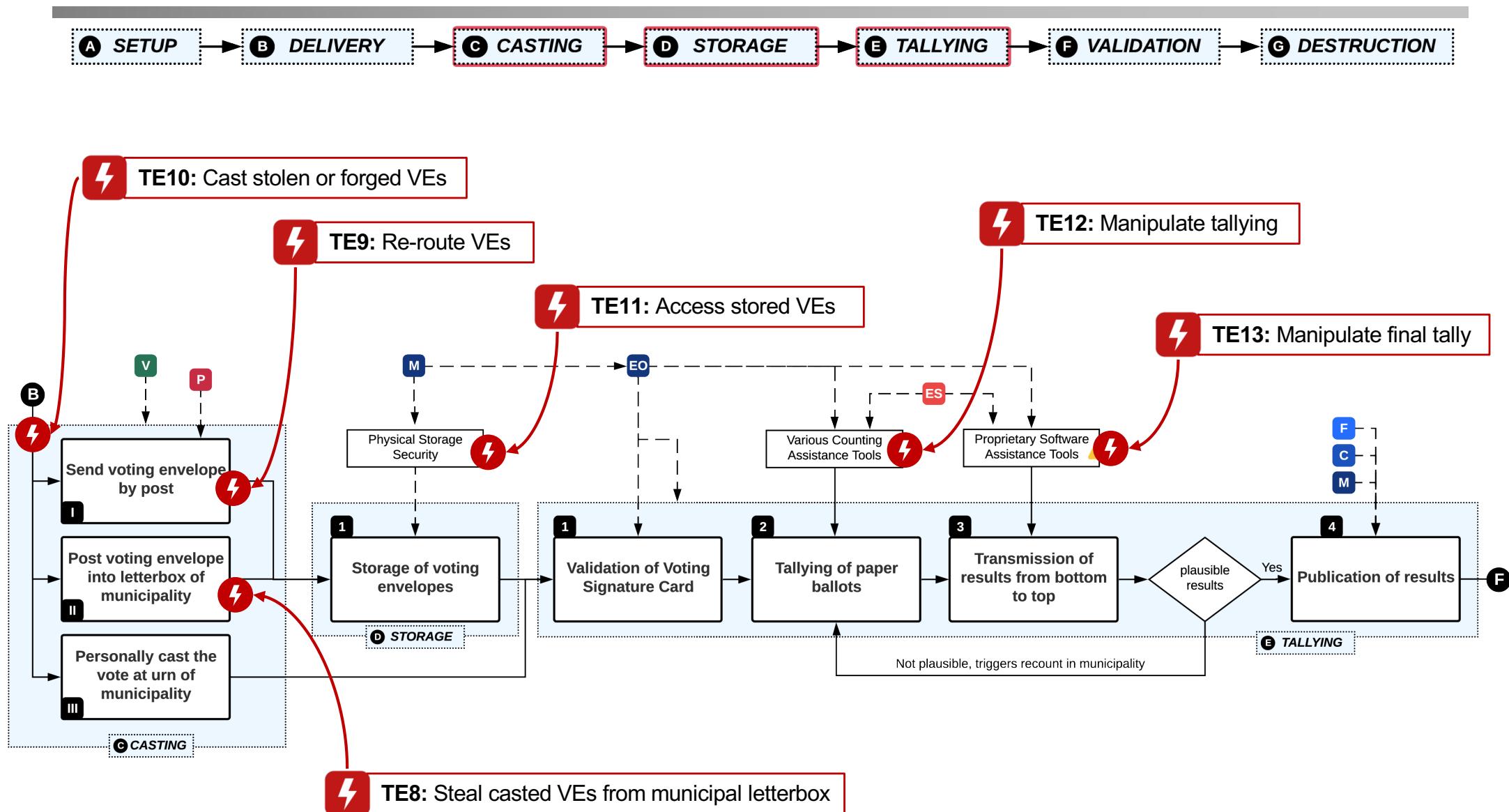
C: Casting, D: Storage, E: Tallying



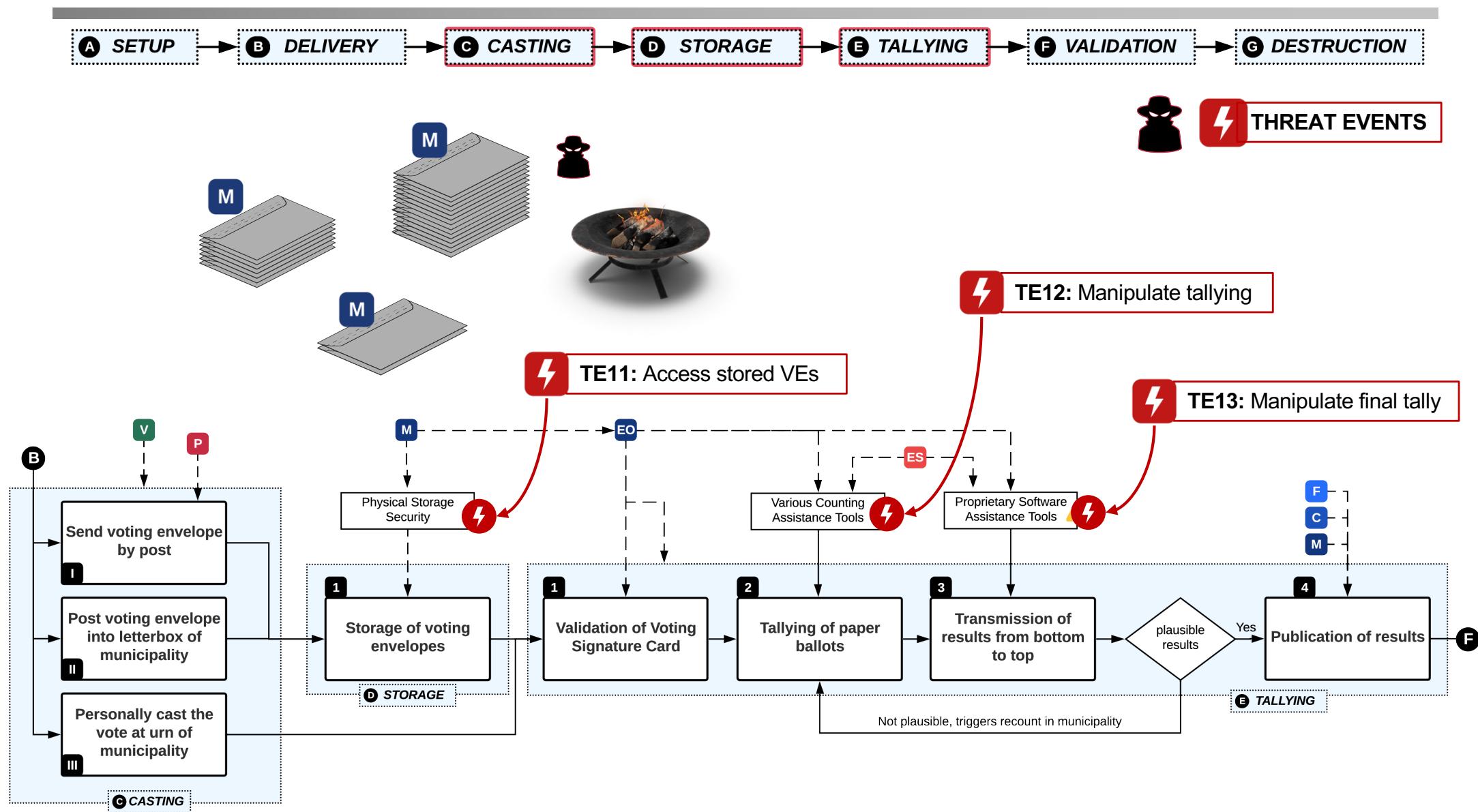
C: Casting, D: Storage, E: Tallying



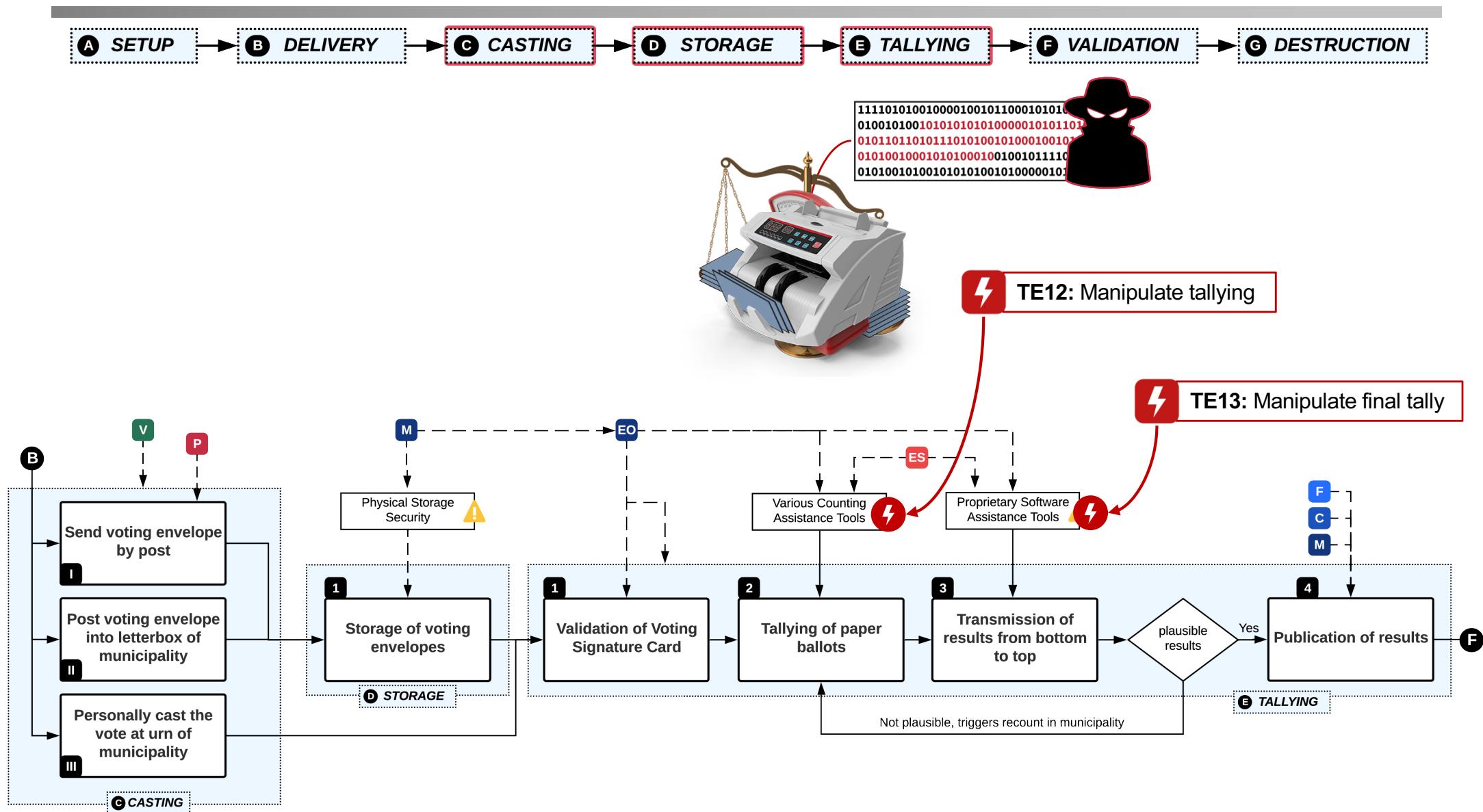
THREAT EVENTS



C: Casting, D: Storage, E: Tallying

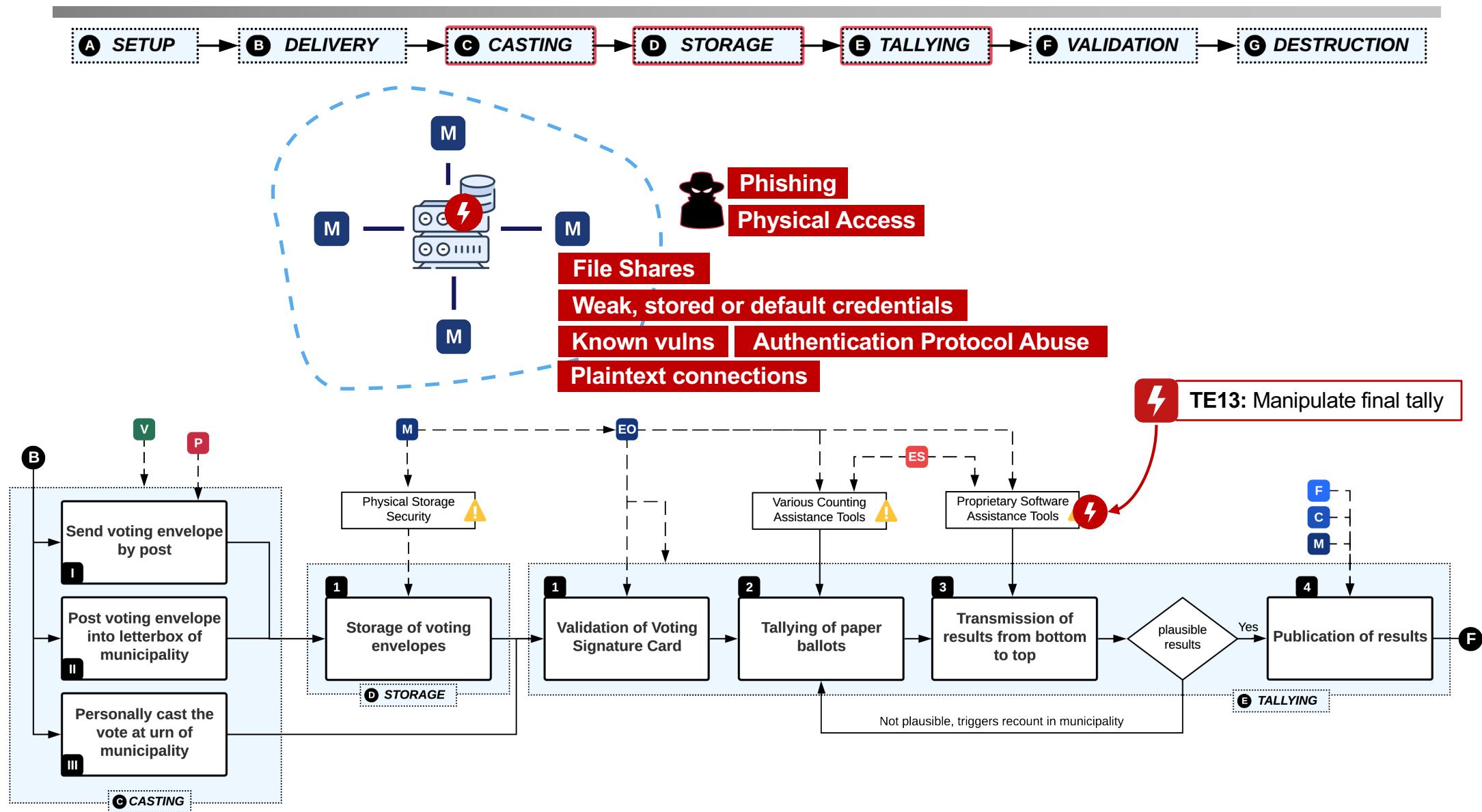


C: Casting, D: Storage, E: Tallying THREAT EVENTS



C: Casting, D: Storage, E: Tallying

THREAT EVENTS



Conclusions on the Swiss RPV

- The Swiss RPV system
 - Heterogeneous process with cantonal variations ☺
 - Substantial trust in third parties ☹
 - Distribution of trust and physical decentralization ☺
- *How can a new design of an electronic voting system distribute trust?*

Remote Electronic Voting (REV)

- REV Requirements and Properties
- Security Building Blocks
 - Homomorphic Encryption, ZKP, PBB

REV Requirements

❑ Privacy

- A vote must not identify a voter and any traceability between the voter and its vote must be removed

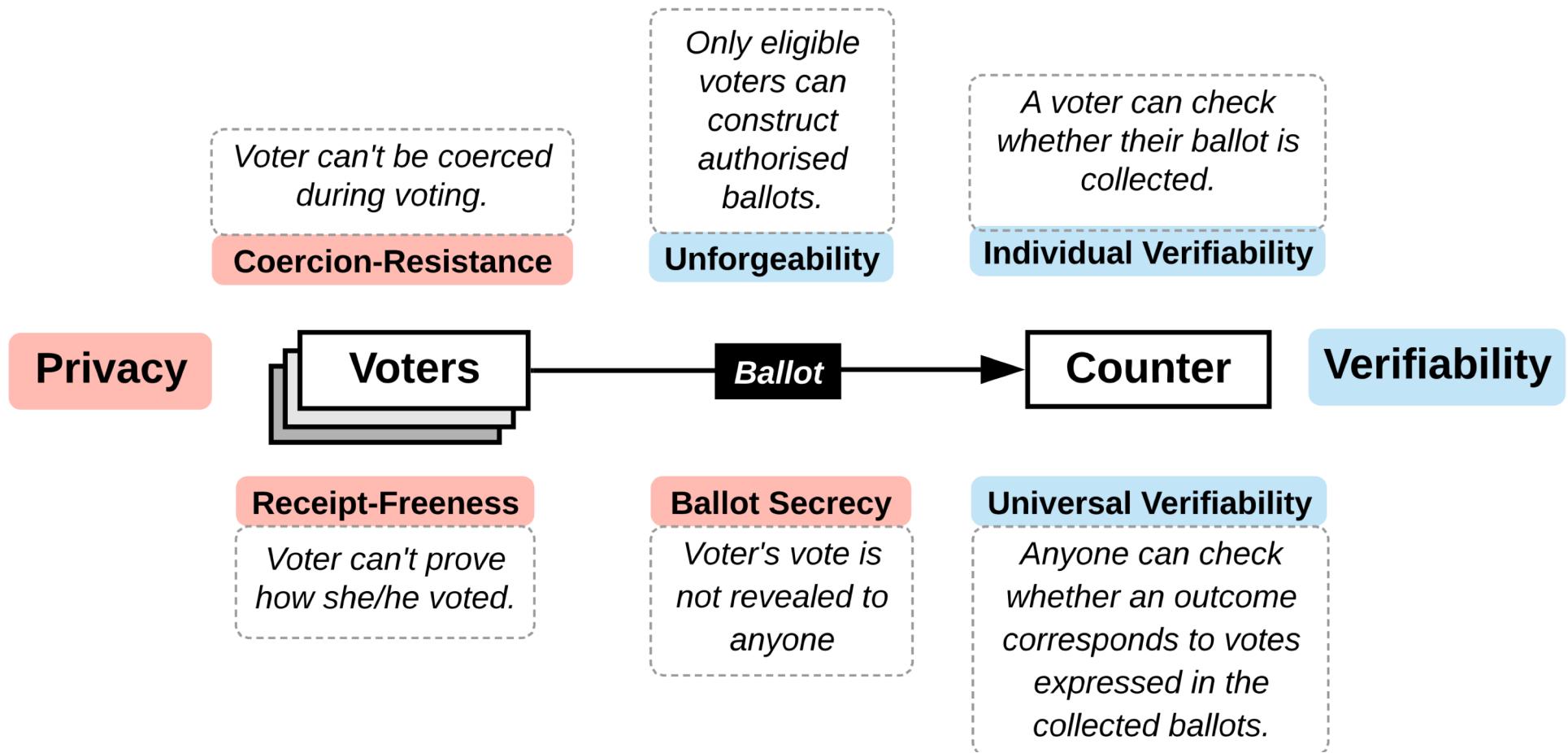
❑ Verifiability

- A voter should be able to verify if its vote was correctly recorded and accounted for in the final vote tally

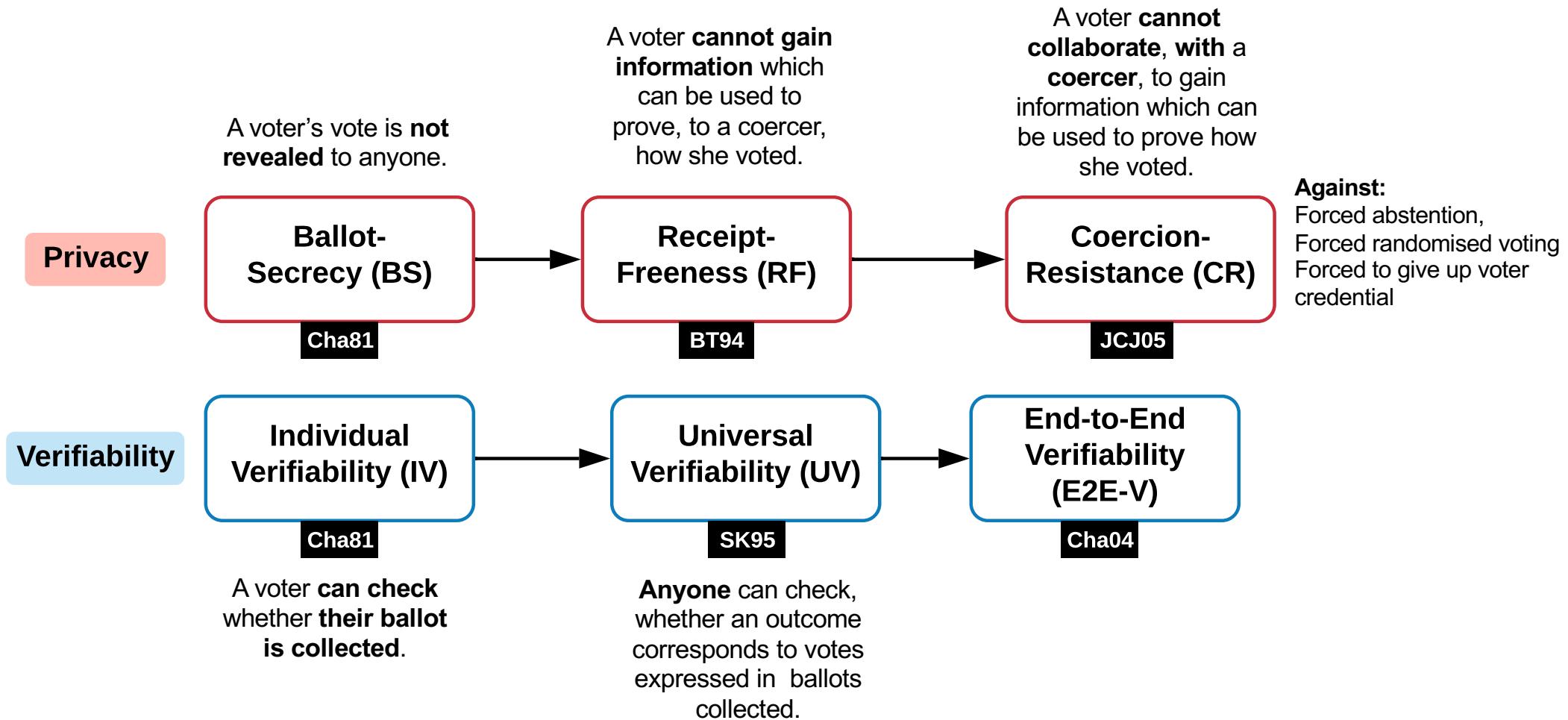
❑ Absolute privacy (no information leaks) cannot coexist concurrently with verifiability (sufficient information leaked to verify the result)

- Goal of voting system design is to find a way to enable as much privacy and verifiability simultaneously as possible

Voting and Electoral Processes

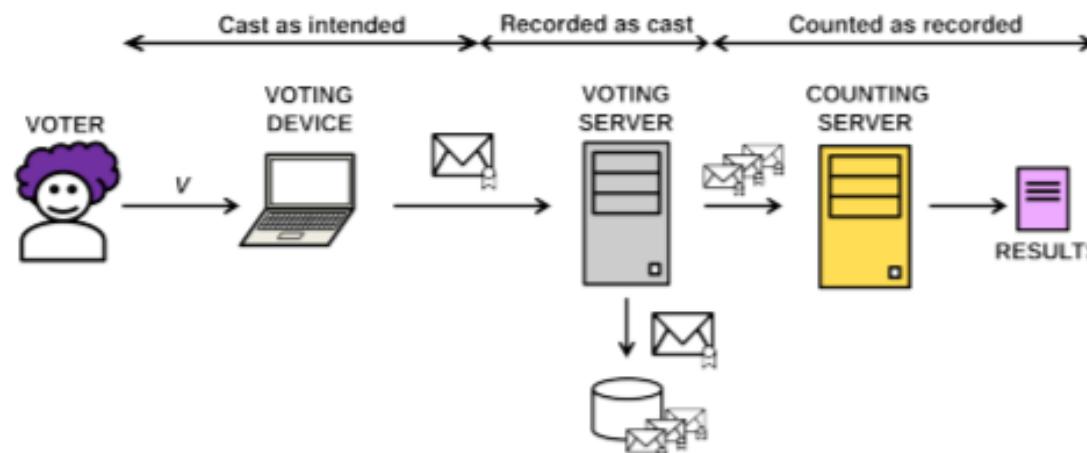


Privacy and Verifiability Notions



End-to-end Verifiability

- End-to-end Verifiability “consist” of:
 - Cast-as-Intended
 - The voter’s choice was correctly denoted on the ballot by the system
 - Recorded-As-Cast
 - The voter’s ballot was received the way she cast it
 - Count As Recorded
 - The Voter’s ballot counts as received



Secret Ballot Voting Schemes

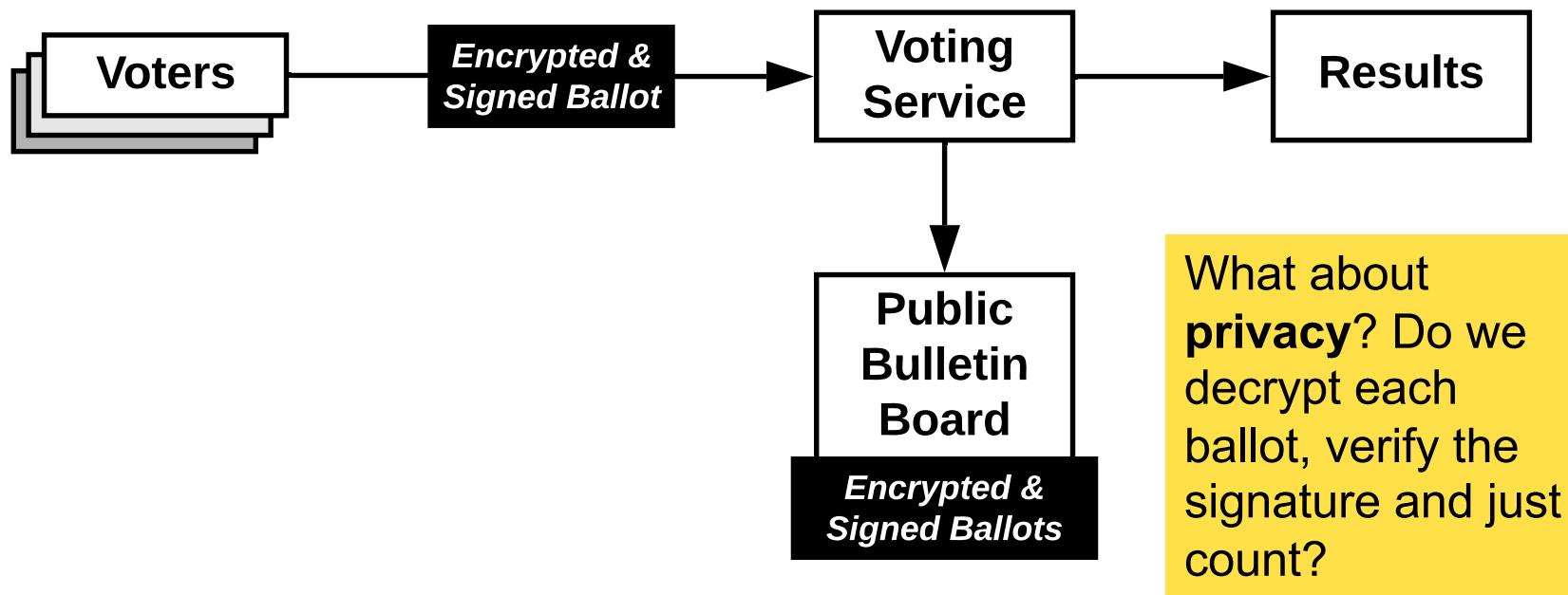
scheme	privacy	verifiability	attacks	based on
FOO92 [32]	BP	UV	KR05 [44]	BS
CGS97 [25]	BP	UV	—	HE
BT94 [15]	RF	—	HS00 [37]	HE
NR94 [58]	RF	—	—	MC
SK95 [68]	RF	UV	MH96 [50]	MN
Oka96 [60]	RF	—	Oka97 [61]	BS
Oka97 [61]	RF	IV, UV	—	BS
HS00 [37]	RF	IV,UV	—	MN
LK00 [46]	RF	UV	LBD04 [45]	HE
BFP01 [8]	RF	UV	Hir01 [36], JCJ05 [42]	HE
MBC01 [48]	RF	—	LK02 [47], JCJ05 [42]	HE
LK02 [47]	RF	UV	—	HE
LBD03 [45]	RF	UV	—	MN
ALBD04 [4]	RF	IV, UV	—	MN
JCJ05 [42]	RF, CR	UV	—	MN
MN06 [52]	EBP*, RF	UV	—	CS
MN07 [54]	EBP*, RF	UV	—	CS, HE

BP: Ballot Privacy
RF: Receipt-Freeness
CR: Coercion-Resistance
EBP: Everlasting Ballot-Privacy
IV: Individual Verifiability
UV: Universal Verifiability

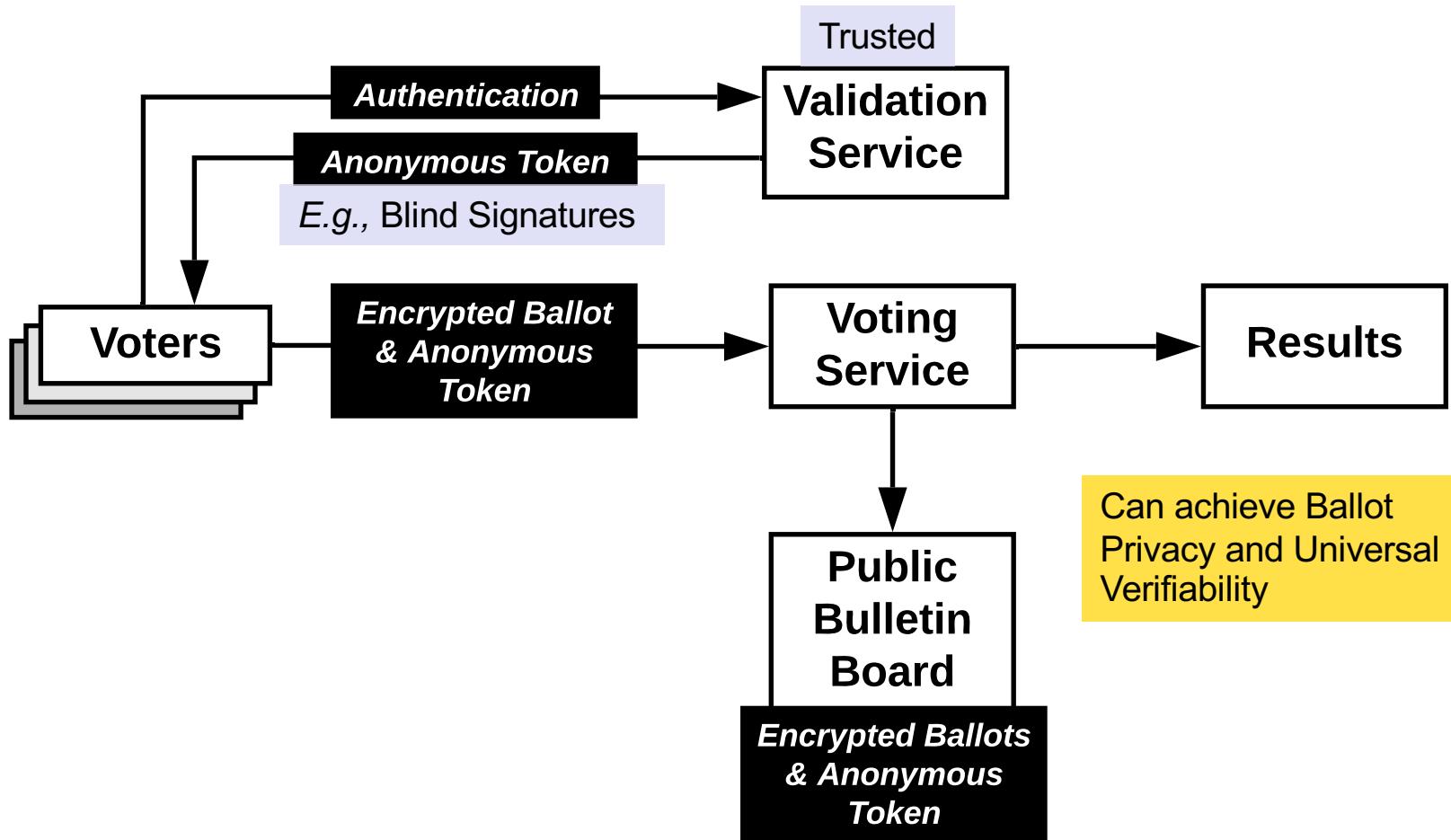
BS: Blind Signatures
HE: Homomorphic Encryption
MC: Multiparty Computation
MN: Mixnet
CS: Commitment Scheme

Based on H. Jonker :
“Privacy and Verifiability in Voting Systems” 2013

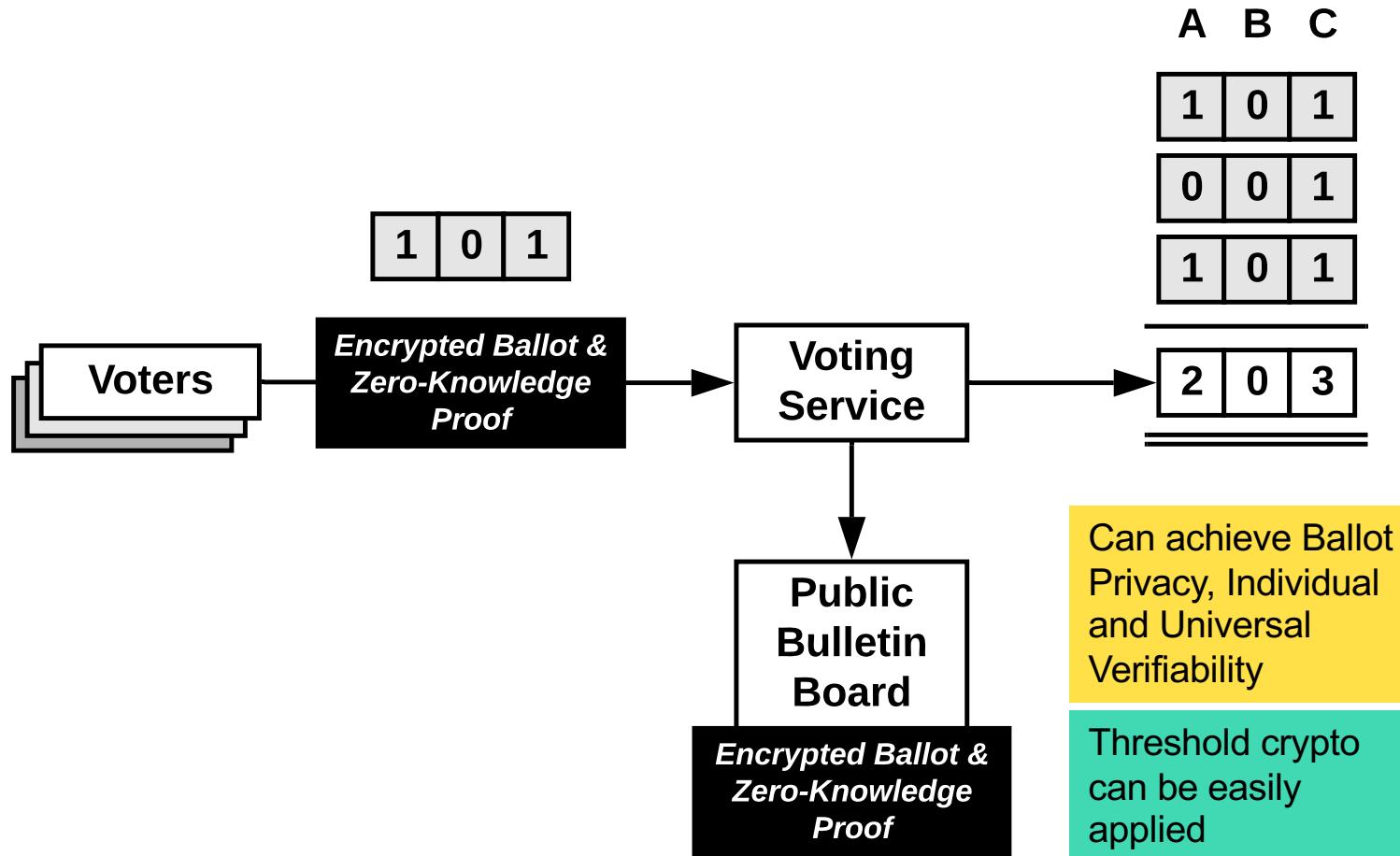
Encrypt and Sign



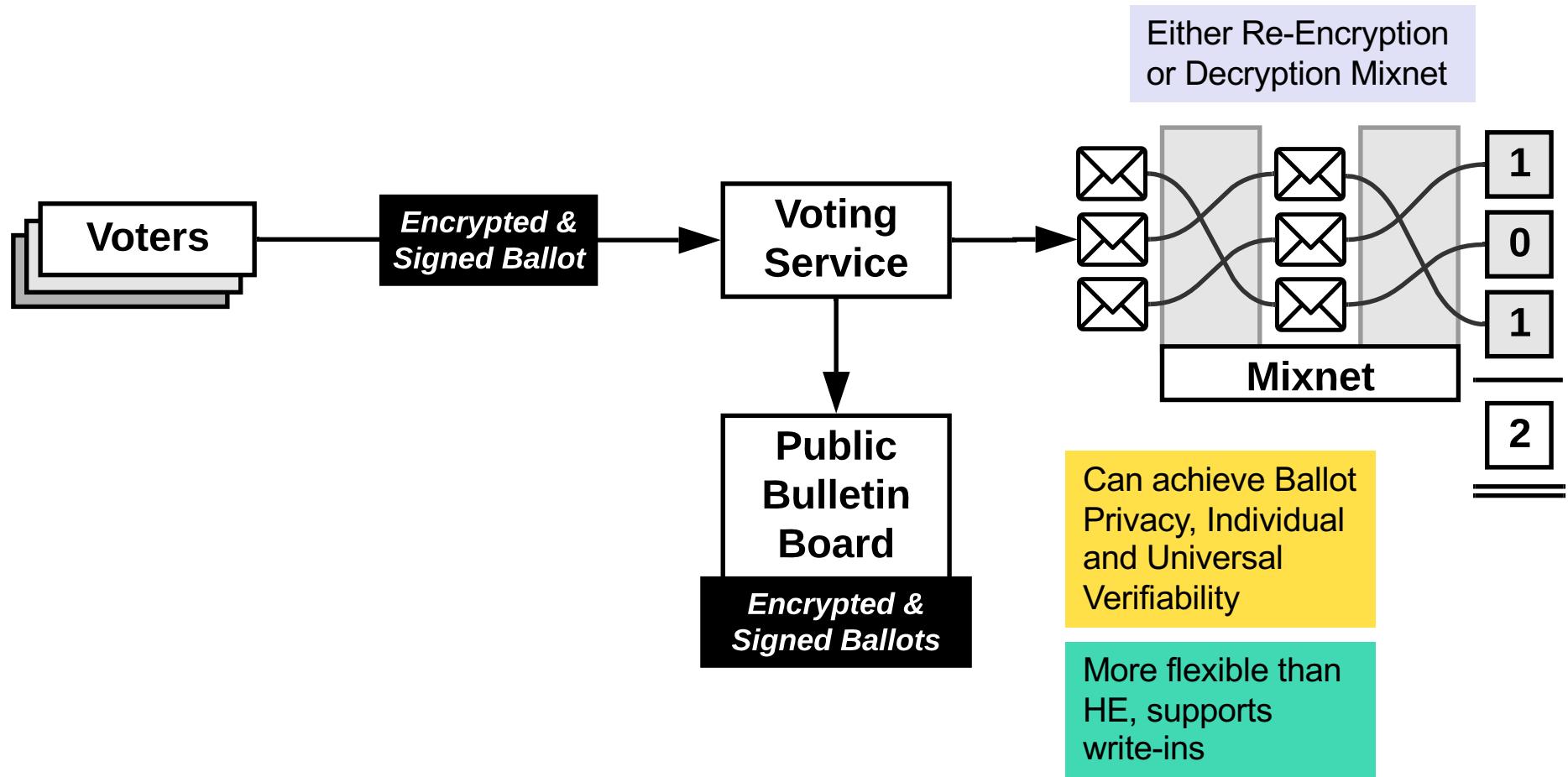
Two Agencies Model



Homomorphic Tallying



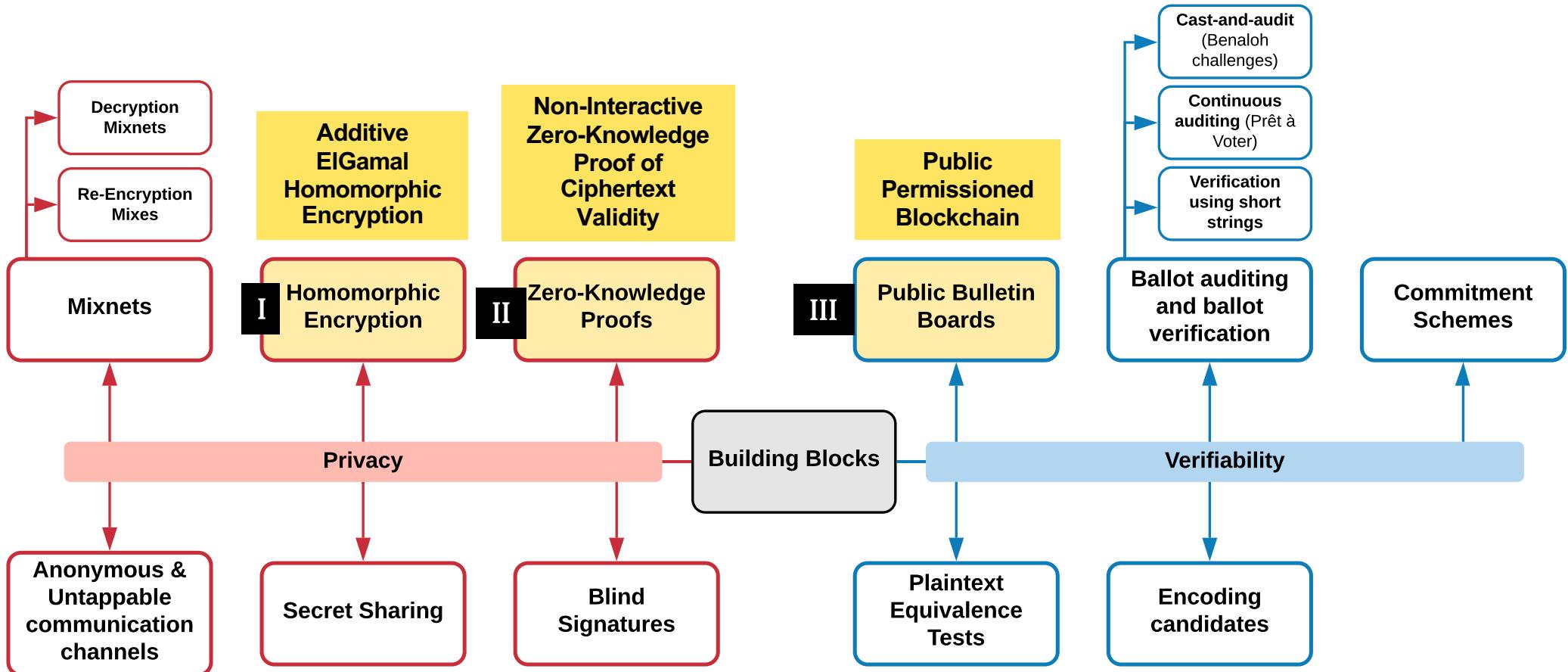
Mixnet



Remote Electronic Voting (REV)

- REV Requirements and Properties
- **Building Blocks**
 - Homomorphic Encryption, ZKP, PBB

Building Blocks for REV Schemes



Homomorphic Encryption I

- In REV, HE used to tally votes
- Every eligible voter V can encrypt his or her $vote$ using the election public key pk , resulting in the encrypted vote: $enc_{pk}(vote_V)$.
- No individual votes need to be decrypted, because the votes can be added together homomorphically.
- Thus, the final, encrypted tally is

$$enc_{pk}(vote_1) \otimes \dots \otimes enc_{pk}(vote_n) = \\ enc_{pk}(vote_1 \oplus \dots \oplus vote_n)$$

A	B	C
1	0	1
0	0	1
1	0	1
2	0	3

Proving Ciphertext Validity

II

- But how encryption malleability tackled?
 - I.e. What happens if 100 instead of 1 is encrypted?
 - In search of a solution to assure the validity of the ciphertext, while assuring Ballot Privacy at the same time
- **Zero Knowledge Proofs!**
 - Each voter proves that she cast a valid vote, without revealing her/his vote
 - Authorities prove that they know their secret keys (that match the election public keys), without revealing their secret keys
 - At the end of the election, authorities prove that they have tallied correctly (decrypted the results correctly), again without revealing their secret keys

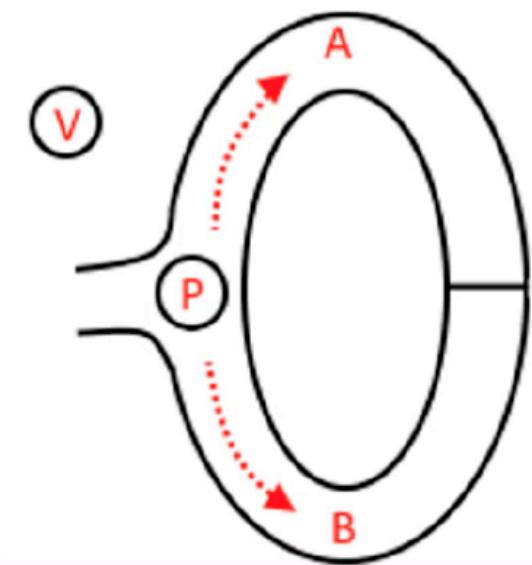
Zero Knowledge Proofs

II

- **Zero Knowledge Proof (ZKP)** is a proof of a statement s which **reveals nothing about statement s , except that it is true**
 - With the use of a ZKP system, a prover P can convince a verifier V via an interaction that some statement s is true.
- **Non-interactive ZKP (NIZKP)**
 - This relies on the prover generating a (to him) unpredictable challenge (which cannot be tweaked) based on his commitment and public knowledge, such as the hash of the commitment.
 - *In REV: NIZKPs enable a voter to verify that her vote is valid, being able to prove to an outsider what she voted.*

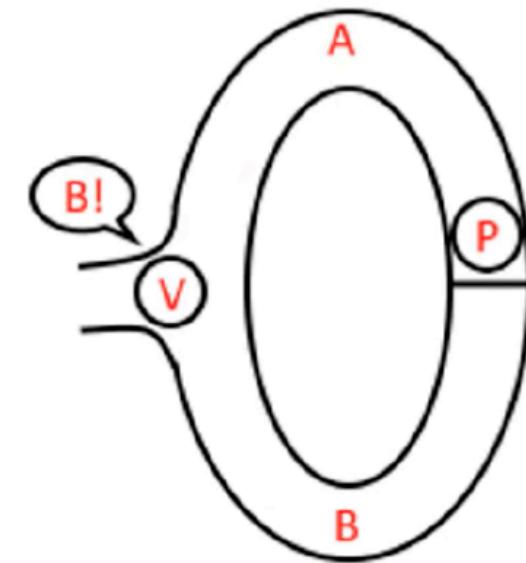
Ali Baba's Cave (1) II

- The cave has a **single entry** and is shaped like a ring with two paths (A and B) and **contains a hidden door separating the two paths**
- Peggy (P – “prover”) knows the password to open the hidden door **but does not want to reveal it**
- To prove to Victor (V – “verifier”) that Peggy knows the password, Peggy enters the cave and chooses a path



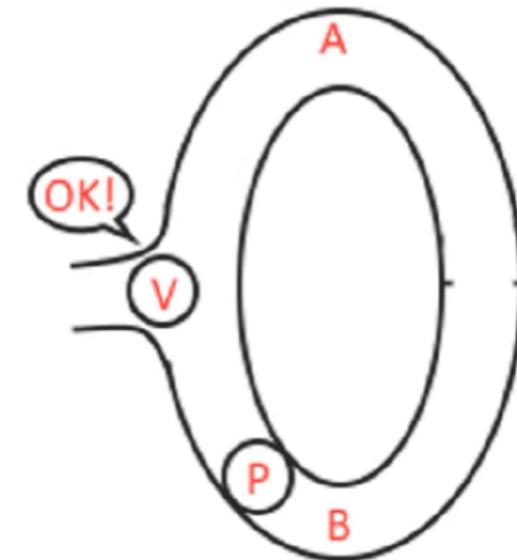
Ali Baba's Cave (2) II

- Next, Victor enters the cave and demands that Peggy exits the cave using path A or B, chosen at random
 - On one hand, since P knows the password, it is trivial for her to pass the test
 - On the other hand, would P had not known the password, she would have had a 50% chance only of returning from the path demanded

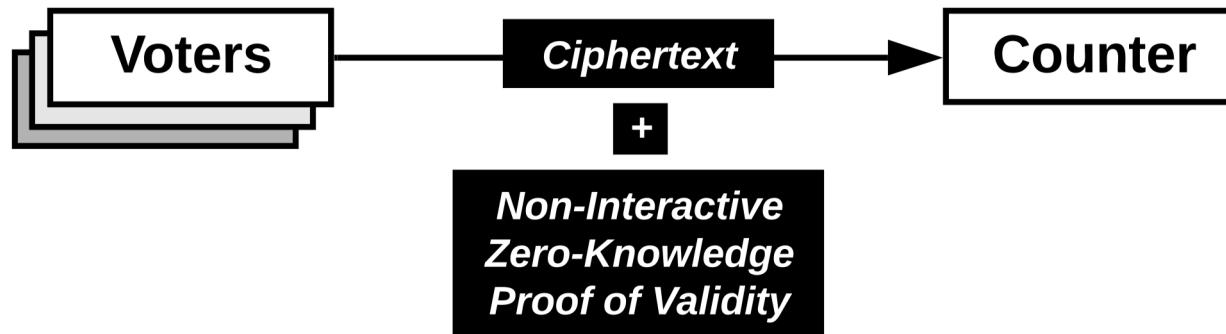


Ali Baba's Cave (3) II

- Victor can challenge Peggy multiple times, thereby, **decreasing the probability** of Peggy being a fraudulent “prover”
 - For each challenge the probability decreases by a factor of two
 - Therefore, Victor can repeat this process as many times as deemed necessary, until the desired level of confidence is obtained



Achieving Privacy with HE and ZKPs II



- Ballot Privacy achieved by encrypting with the public election key, and proving validity with NIZKPs
 - Thus, no individual ballot needs to be decrypted and authorities keep their secret election keys private, while homomorphically tallying the final result

➤ *How can voters verify election data?*

Public Bulletin Board (PBB) III

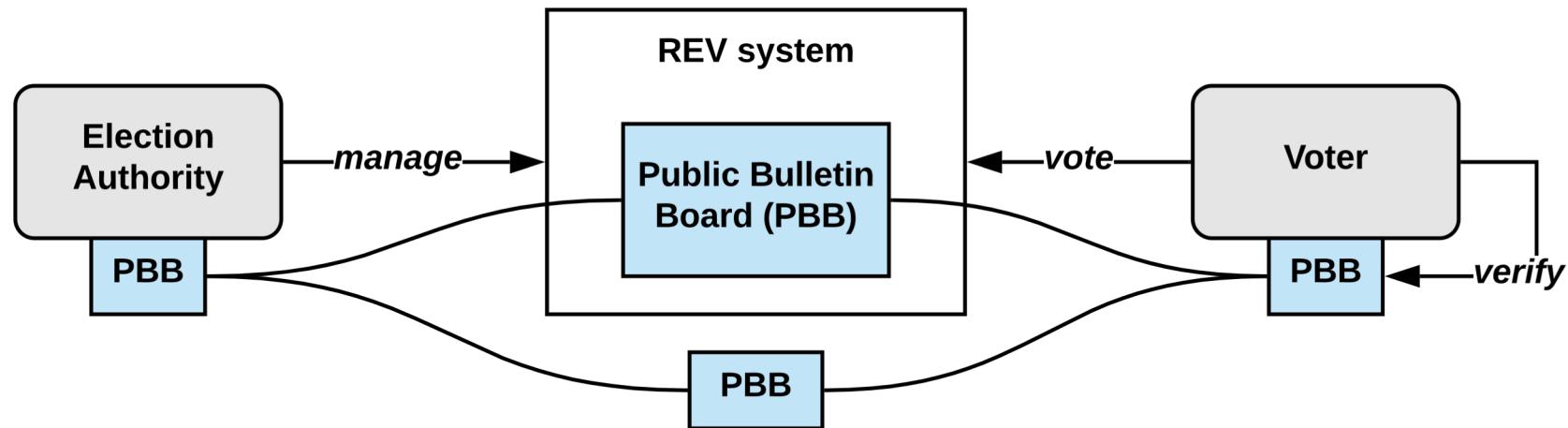
- PBB serving as a
 - (1) **shared, append-only** data structure
 - (2) **public** and searchable by anyone
 - (3) **consistent** view for anyone accessing its information
- In practice, a **public permissioned Blockchain (BC)** fulfills those theoretical requirements

[KRM20]

Public Permissioned Blockchain (BC) III

□ Deployment of a Public Permissioned BC

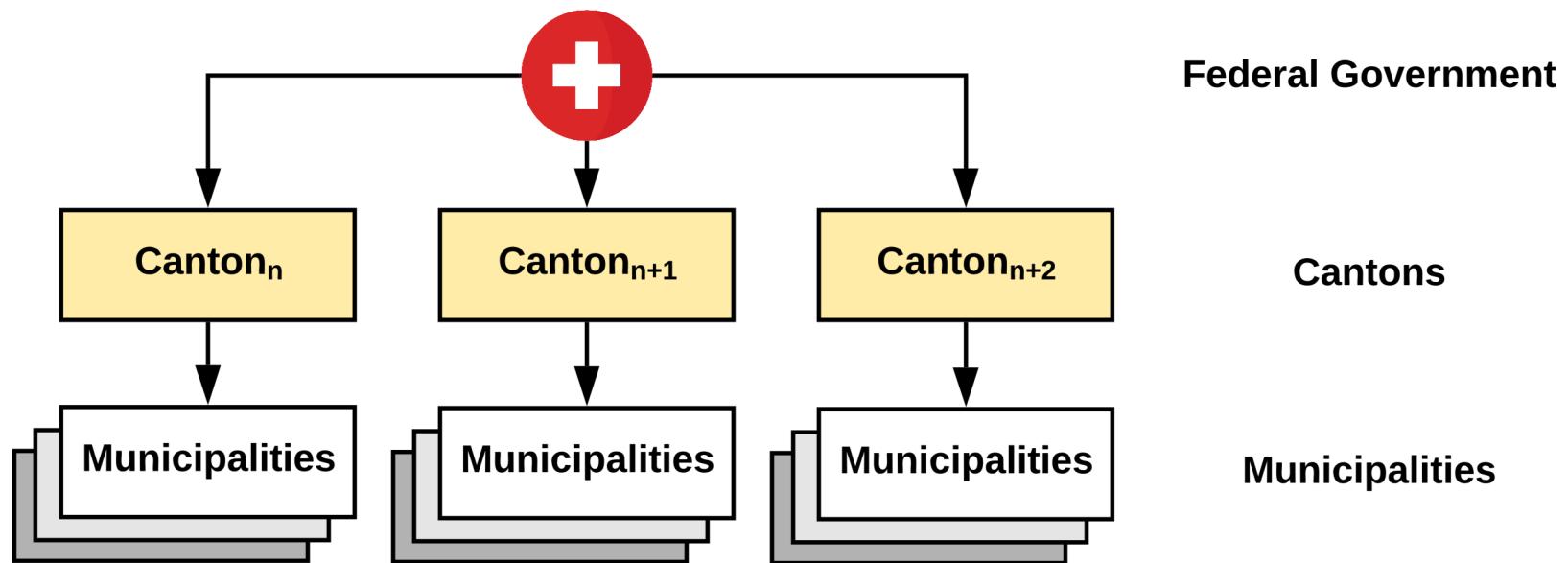
- Read operations: Public
- Write operations: Permissioned



[KRM20]

The Swiss Scenario

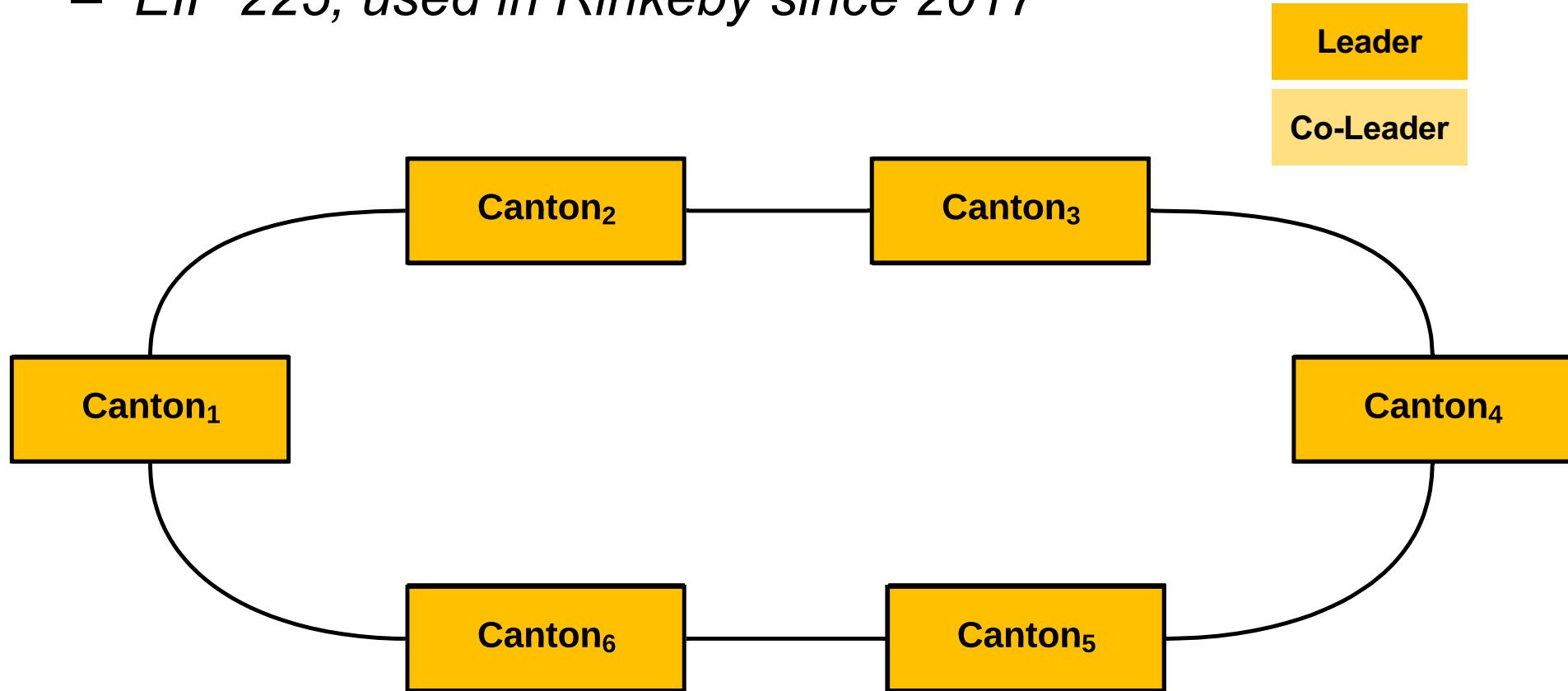
- The Federalism of Switzerland serves as a suitable framework for a **decentralized** BC-based REV system



[KRM20]

Proof-of-Authority (PoA) Consensus

- Consensus Algorithm: Clique Proof-of-Authority (PoA)
 - *EIP 225, used in Rinkeby since 2017*



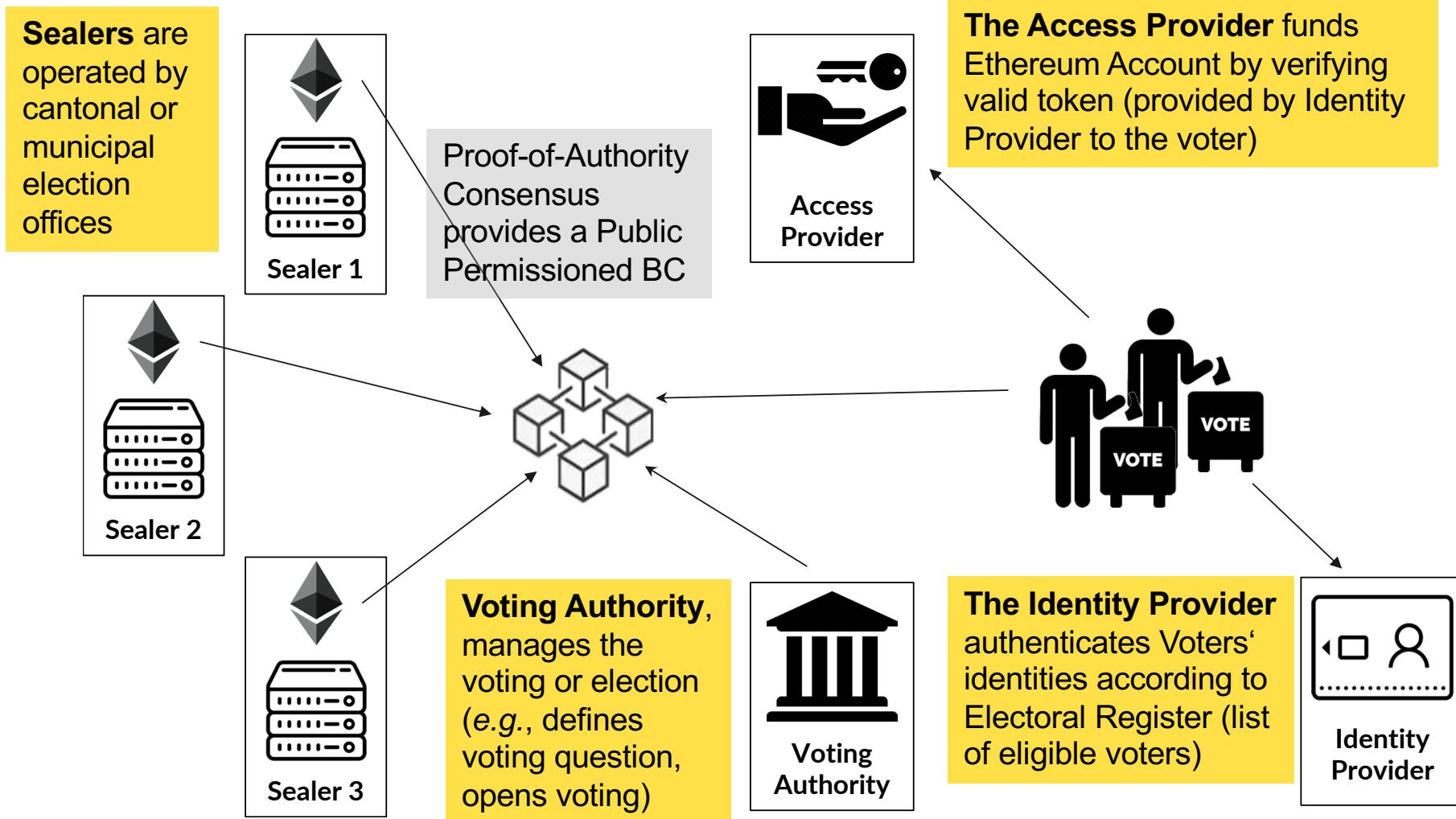
Blockchain-based REV

- Instructions for local deployment (Practical Part)
- **Provotum Stakeholders, Voting Protocol and Evaluations**

Blockchain-based REV

- Instructions for local deployment (Practical Part)
- **Provotum Stakeholders, Voting Protocol and Evaluations**

BC-based REV System: *Provotum*



Voting Protocol: Registration (1)

Voting Authority

OFF CHAIN 

1 REGISTRATION
2 PAIRING
3 KEY GENERATION
4 VOTING
5 TALLYING
6 RESULT

Address Registration

Each sealer has an Ethereum account. This account consists of a public and private key. The public key represents the address of the holder within the network (also known as Wallet). In this step, each sealer will register its wallet address with the authority.

 currently 0/3 sealers are registered

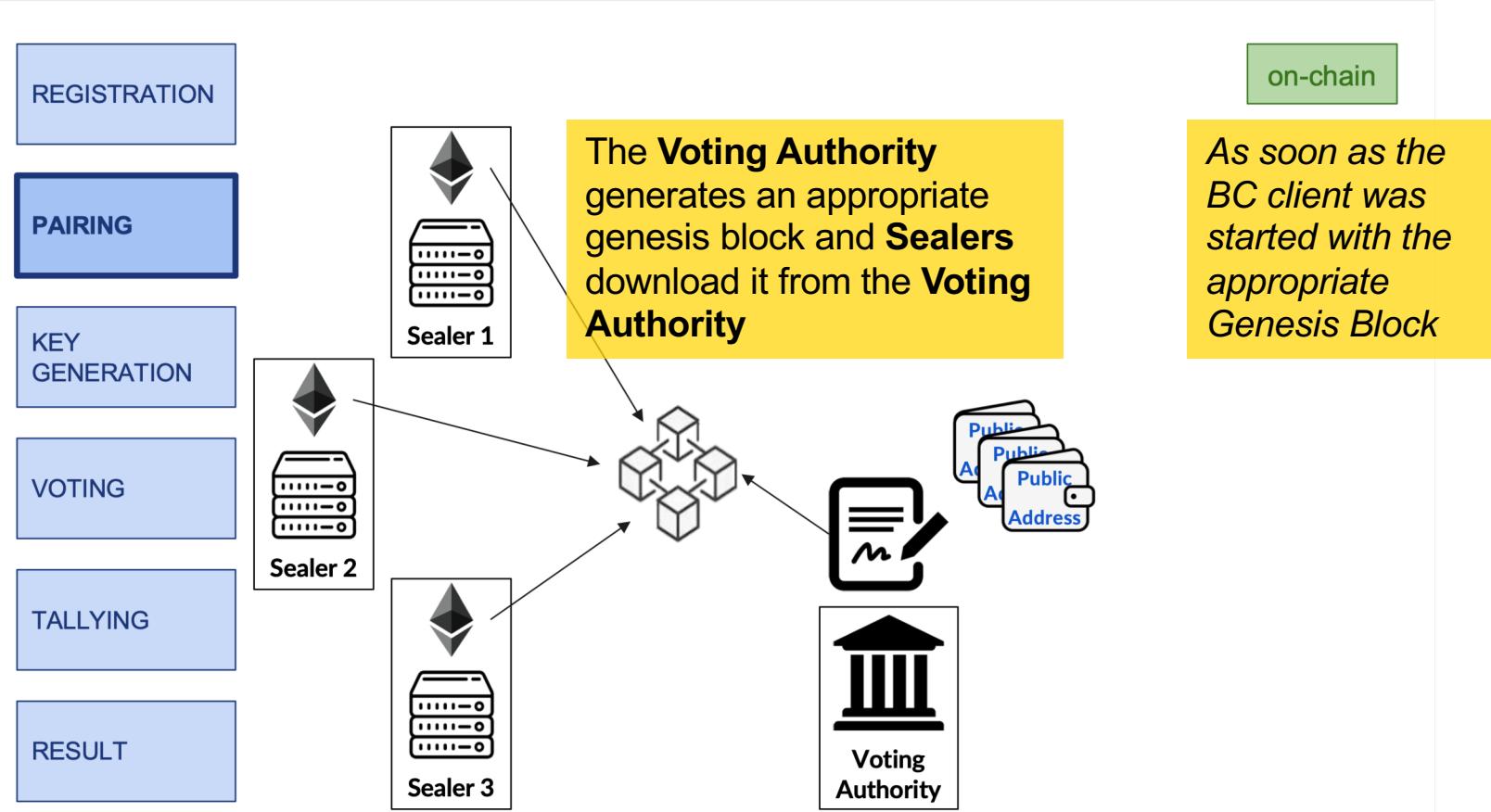
 please wait until all sealers have registered their address

[NEXT STEP](#)

Copyright © Nik Zaugg Alex Scheitlin Moritz Eck 2020.

Voting Protocol: Pairing (2)

PoA Bootstrapping, where the appropriate Genesis Block is retrieved from the Voting Authority



Voting Protocol: Pairing (2)

Voting Authority

OFF CHAIN 

- 1 REGISTRATION
- 2 PAIRING
- 3 KEY GENERATION
- 4 VOTING
- 5 TALLYING
- 6 RESULT

Network Pairing

A sealer will act as a validator on the Proof of Authority (PoA) blockchain. In order to start the blockchain, each sealer will have to boot one parity node with the provided chain specification. All parity nodes run by the sealers will form the PoA blockchain. Before a contract can be deployed, each sealer will need to register with the Voting Authority.

↔ currently 0/3 sealers have signed up

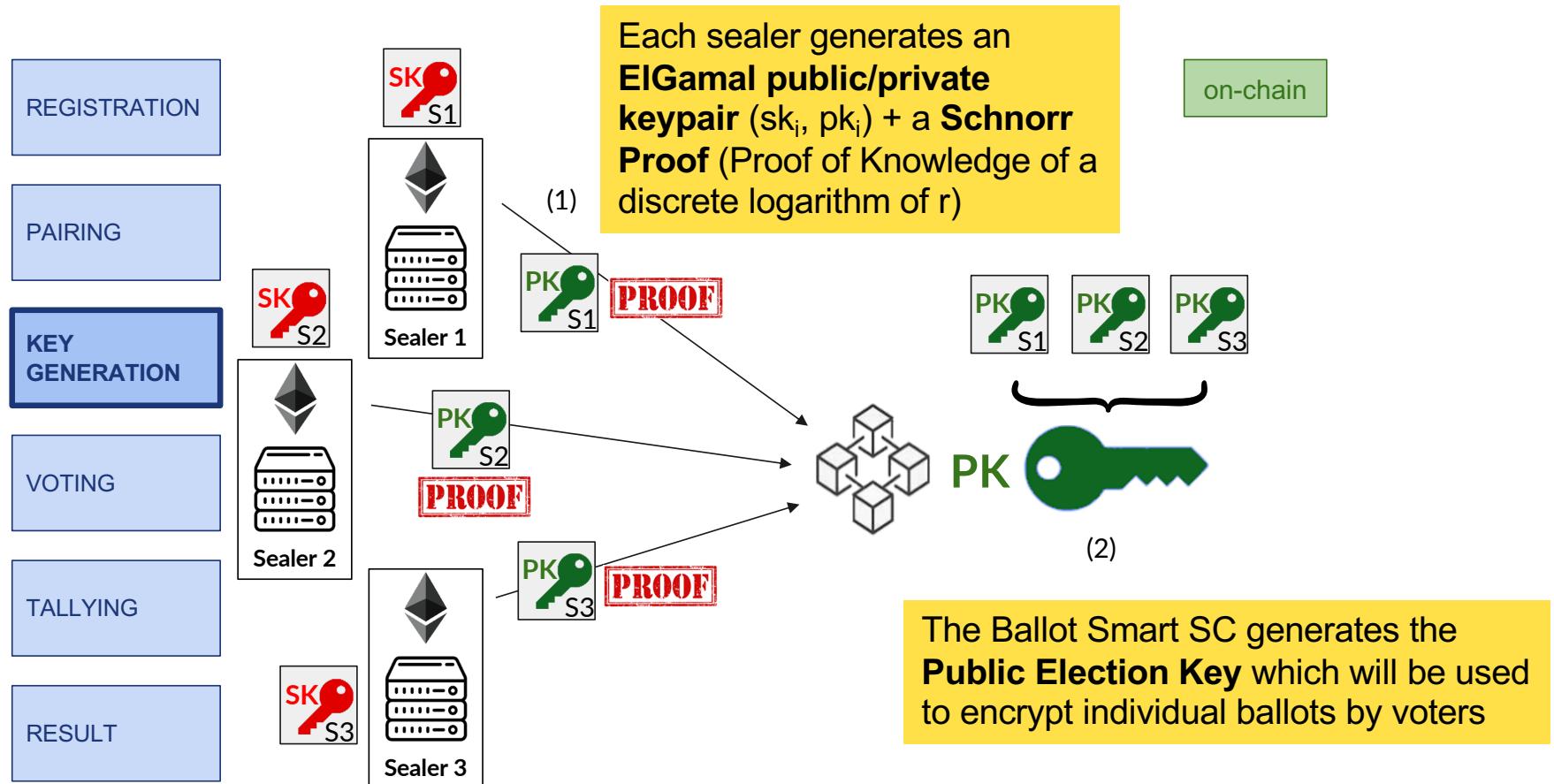
please wait until all sealers have registered to deploy the contract

Enter Vote Question *

NEXT STEP >

Copyright © Nik Zaugg Alex Scheitlin Moritz Eck 2020.

Voting Protocol: Key Generation (3)



Voting Protocol: Key Generation (3)

Voting Authority

ON CHAIN

- ✓ REGISTRATION
- ✓ PAIRING
- 3 KEY GENERATION
- 4 VOTING
- 5 TALLYING
- 6 RESULT

Key Generation

Each sealer will generate a public and private key share. The public share will be submitted to the Ballot Smart Contract. The combination of the public key shares will then form the final public key of the system. The Voting Authority will trigger the creation of the public key.

0/3 public key shares have been submitted

waiting for all key shares to be submitted

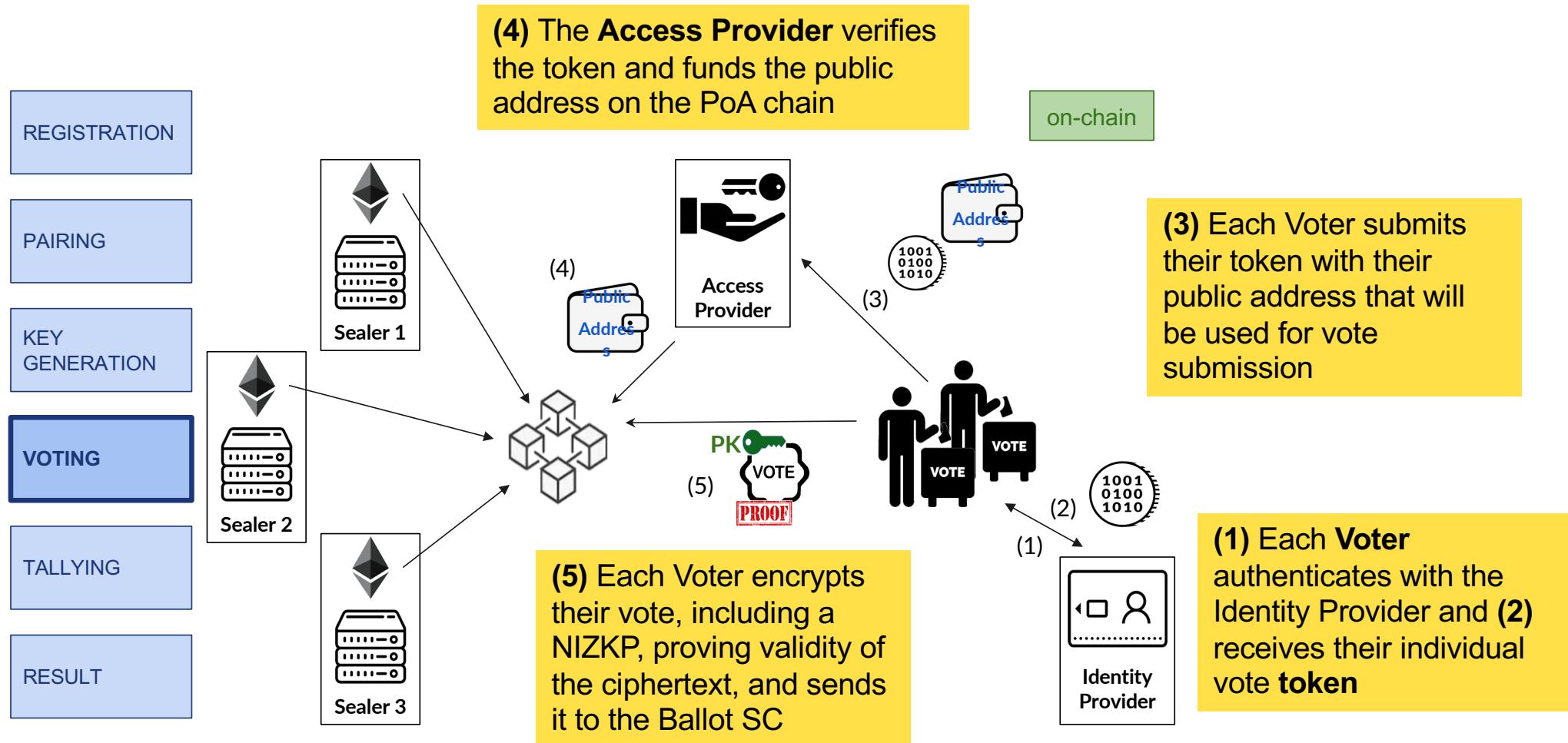
GENERATE PUBLIC KEY

OPEN VOTE

1

Copyright © Nik Zaugg Alex Scheitlin Moritz Eck 2020.

Voting Protocol: Voting (4)



Voting Protocol: Voting (4)

Voting Authority

ON CHAIN 

- ✓ REGISTRATION
- ✓ PAIRING
- ✓ KEY GENERATION
- 4 VOTING
- 5 TALLYING
- 6 RESULT

Voting

We are in the voting phase. The Voting Authority can decide when to close the vote, this will also trigger a state change in the Ballot Smart Contract. After the vote is closed, no more votes can be submitted.

 Is Vanilla better than Chocolate?

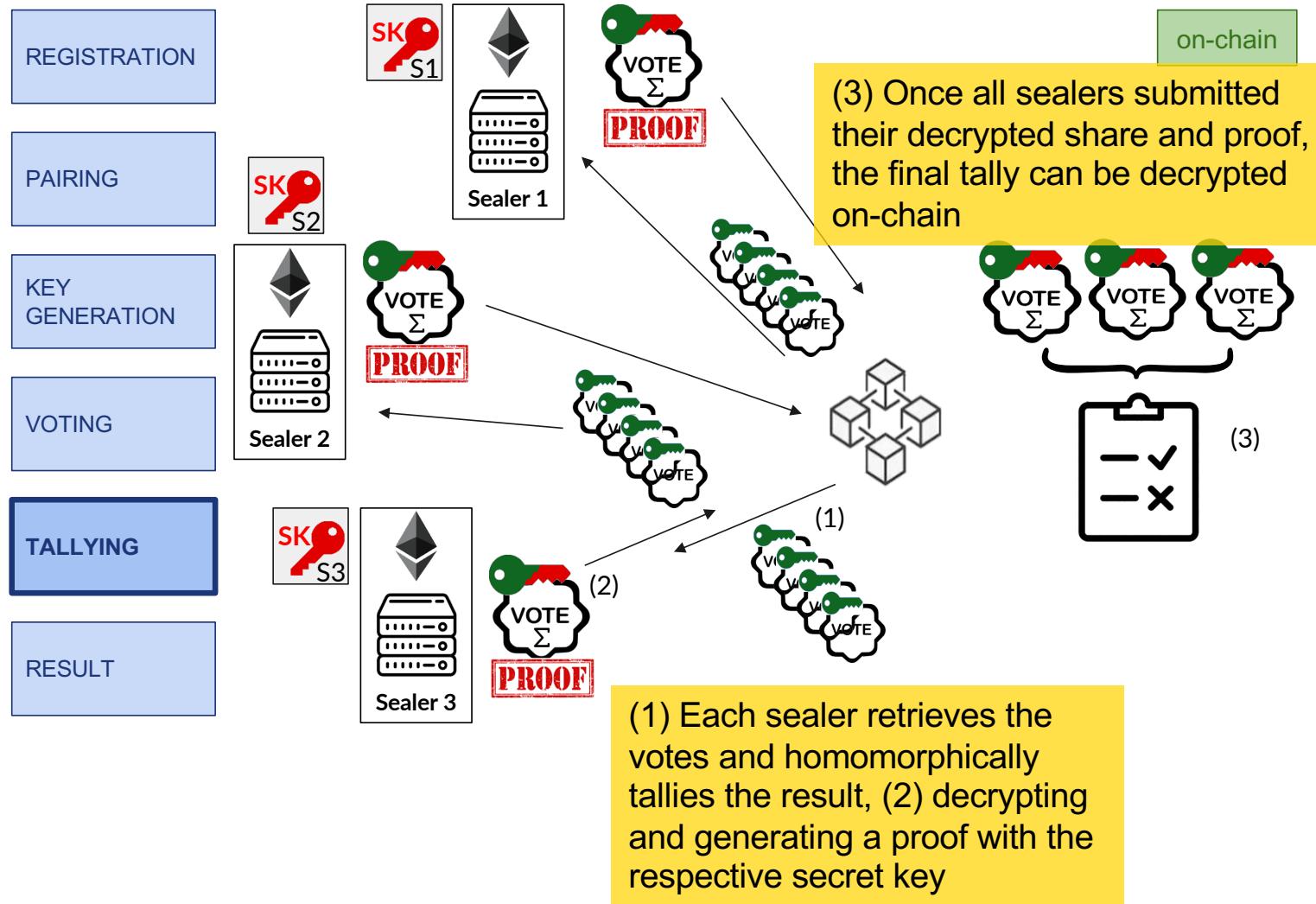
 0 - votes submitted

The vote is currently ongoing. Press the button below to end the vote. After closing the vote, no voters can submit votes anymore. This action cannot be reverted!

[CLOSE VOTE](#)

Copyright © Nik Zaugg Alex Scheitlin Moritz Eck 2020.

Voting Protocol: Tallying (5)



Voting Protocol: Tallying (5)

The screenshot shows a user interface for a Voting Authority. At the top, there's a navigation bar with the text "Voting Authority" and "ON CHAIN" next to a circular icon. On the left, a vertical sidebar lists six steps: "REGISTRATION" (checked), "PAIRING" (checked), "KEY GENERATION" (checked), "VOTING" (checked), "TALLYING" (number 5), and "RESULT" (number 6). Below the sidebar, the main area is titled "Tallying". It contains a descriptive text about the process of tallying votes using a Ballot Smart Contract. To the right of the text, there's a status indicator: "0/3 decrypted shares submitted" with a note below it: "waiting until all decrypted shares have been submitted." At the bottom of the main area is a button labeled "GENERATE SUMMARY". At the very bottom of the page, there's a copyright notice: "Copyright © Nik Zaugg Alex Scheitlin Moritz Eck 2020."

Voting Authority

ON CHAIN

REGISTRATION

PAIRING

KEY GENERATION

VOTING

5 TALLYING

6 RESULT

Tallying

To tally all votes, each sealer node will fetch all ciphers of the votes from the Ballot contract. The sealer will then homomorphically add the vote-ciphers and decrypt the sum, which will be referred to as a decrypted share. Once all decrypted shares are submitted, the Voting Authority can trigger the tallying of the final result in the Ballot Smart Contract.

0/3 decrypted shares submitted

- waiting until all decrypted shares have been submitted.

GENERATE SUMMARY

Copyright © Nik Zaugg Alex Scheitlin Moritz Eck 2020.

Takeaways Provotum

- REV systems require utmost scrutiny to achieve
 - Highly demanding properties of
 - Privacy, Verifiability, Software Independence, Fairness
 - But not limited to
 - Open aspects still include
 - Usability or legal compliance
- Leap from theory to practically deployable REV systems is significant and hard to achieve
 - More research is required to evaluate the viability of establishing such a Public Permissioned Blockchain for on-chain distribution of trust across the voting protocol

Evaluations Provotum 2.0

- ❑ E2E-Verifiability and Ballot Secrecy achieved ✓
 - ❑ Client-Side Cryptography ✓
 - ❑ On-Chain Proof Verification ✓
 - ❑ Distributed Key Generation ✓
 - ❑ Cooperative Decryption ✓
-
- ❑ Key-Size (256-bit) not secure ✗
 - ❑ Mitigate Identity provisioning scheme threats ✗
-
- ❑ Receipt-Freeness and Coercion-Resistance ✗

Summary

Observations

- REVs are country-specific
 - Mainly due to local legislation
- REVs overall system requirements are comparable
 - Privacy and verifiability (cannot coexist in full at the same time)
 - Fairness, eligibility verifiability, and unforgeability
 - Software independence
- REVs building blocks: strong security mechanisms
 - Secret-Ballot Voting Schemes, *i.e.*, voting protocols
 - Cryptographic Primitives, *i.e.*, privacy and verifiability procedures
 - Public Bulletin Board (PBB), *i.e.*, ballot box for results/logs
- From theory to practical systems – a long way to go!

Considerations

- Remote Electronic Voting
 - If trust is distributed in REV, then REVs can offer better privacy and verifiability than traditional voting channels, under certain trust and computational hardness assumptions
 - As soon as a system is public, future adversaries may be able to decrypt cipher-text
- Achieving such trust distribution can be implemented by using a Public Permissioned Blockchain, where authorities collaborate with a Proof-of-Authority (PoA) consensus mechanism

Thanks for your attention



Questions

References

- [KRM20][Peer-Reviewed, Full Paper] **C. Killer**, B. Rodrigues, R. Matile, E. Scheid, B. Stiller: *Design and Implementation of Cast-as-Intended Verifiability for a Blockchain-based Voting System*. In: Proceedings of the 2020 ACM Symposium on Applied Computing. SAC '20, Association for Computing Machinery, New York, NY, USA, 2020. Paper: <http://bcbev.ch/uciv>
- [KS19][Peer-Reviewed, Full Paper] **C. Killer**, B. Stiller: *The Swiss Postal Voting Process and Its System and Security Analysis*. In: R. Krimmer, M. Volkamer, V. Cortier, B. Beckert, R. Küsters, U. Serdült, D. Duenas-Cid (eds.) Electronic Voting. Springer International Publishing, Cham, 2019, p. 134–149, Paper: <http://pvpf.ch/paper>
- [MK18][Master's Project] R. Matile, **C. Killer**: *Privacy, Verifiability, and Auditability in Blockchain-based E-Voting*, 2018, Master's Project, University of Zurich, <http://bcbev.ch/pv>

Relevant Links to Slides and Code

- To follow along the practical steps on your own system or virtual server, please refer to the **guide** provided at
 - <http://bcbev.ch/ddib20>
- To take a look at the **slides**, please refer to
 - <http://bcbev.ch/ddib20slides>
- To take a look at the **videos**, please refer to
 - <http://bcbev.ch/ddib20videos>