
Blockchain-based Remote Electronic Voting



**Universität
Zürich** ^{UZH}



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
 - Security Building Blocks
 - Homomorphic Encryption, ZKP, PBB
- ❑ BC-based REV
 - Provotum Voting Protocol and Evaluation
- ❑ Summary

Electronic Voting



❑ 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



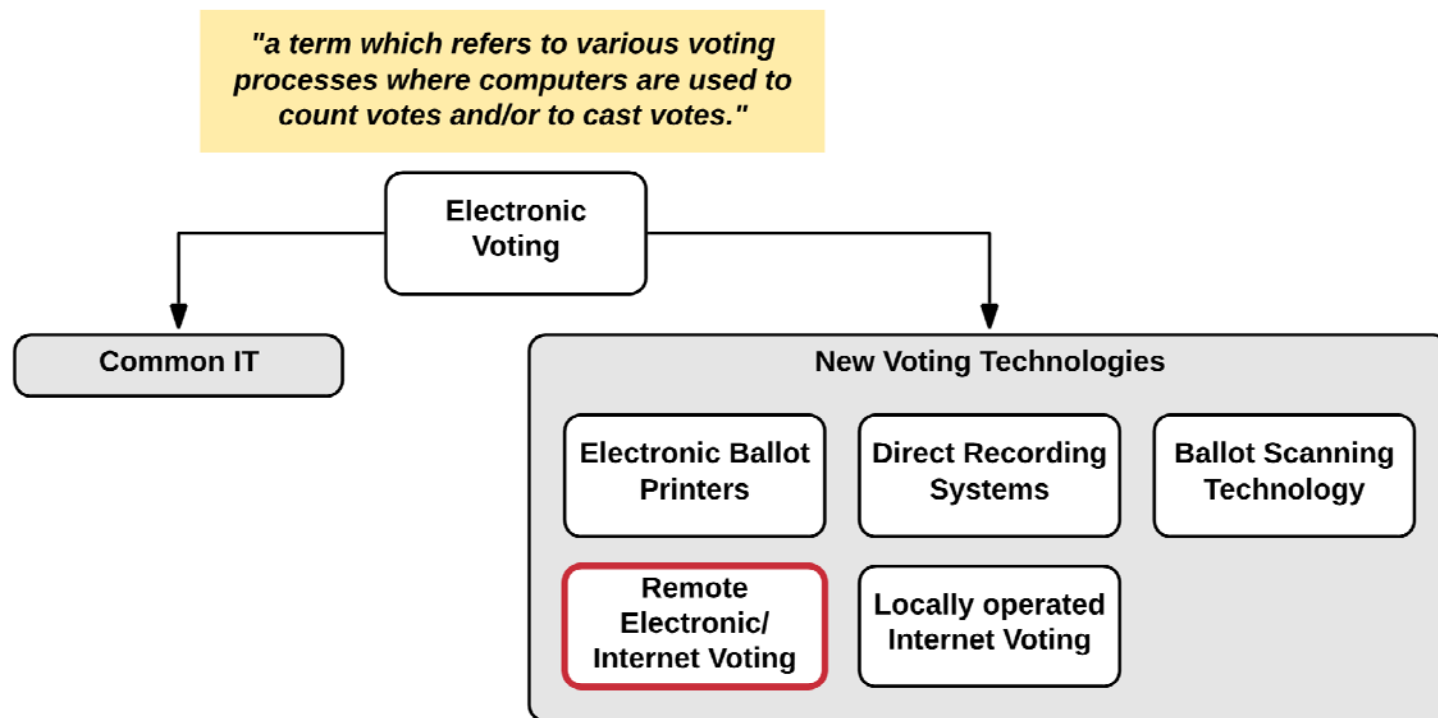
Voters would sometimes be threatened with violence to make sure they backed the right candidate



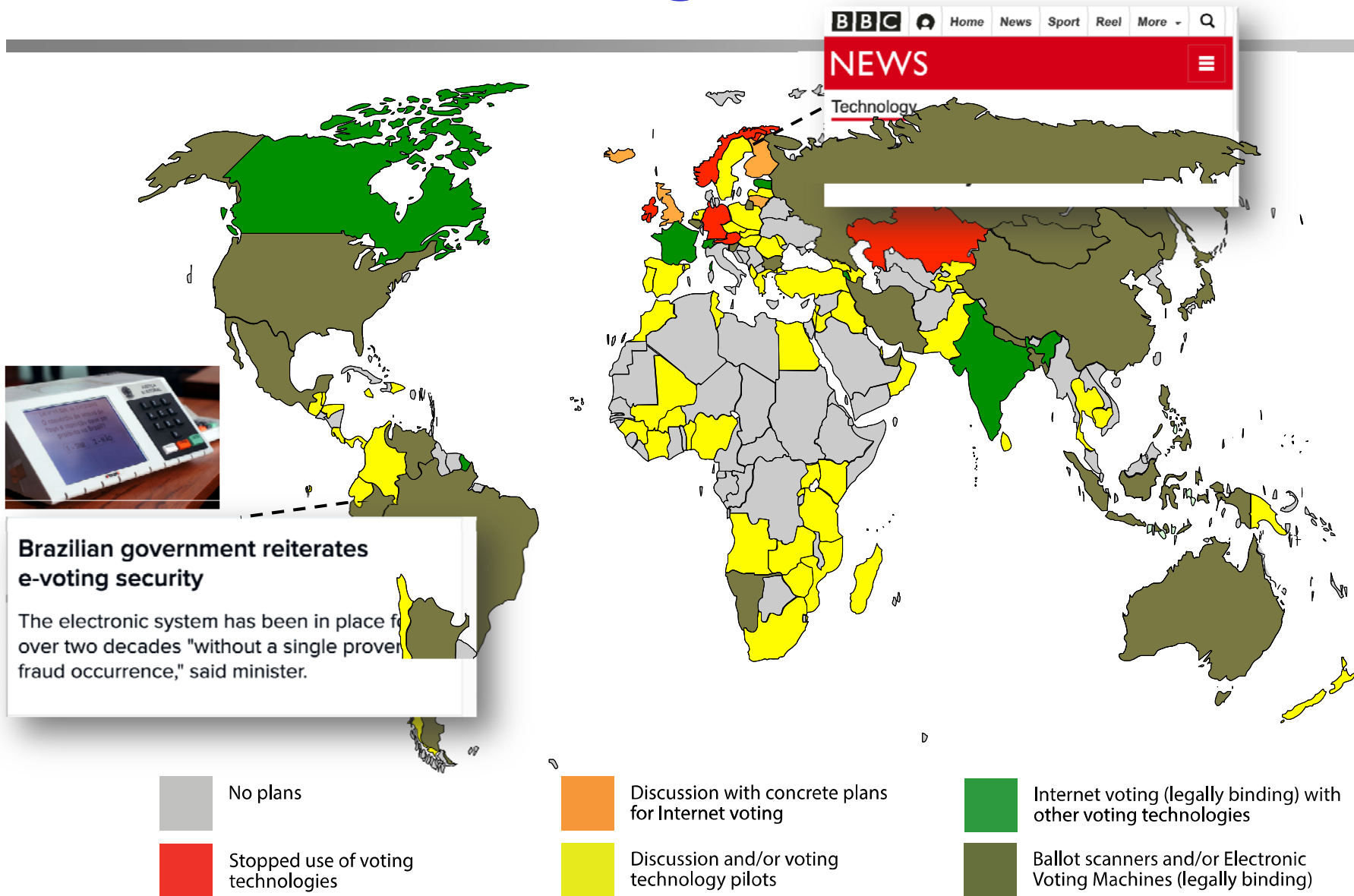
THE GENERAL ELECTION-LEADS FROM OUR ARTIST'S NOTE

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



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

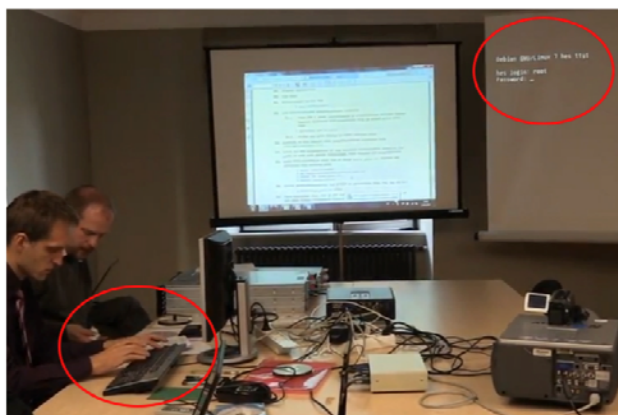


Figure 7: **Keystrokes reveal root passwords** — Videos posted by officials during the election show operators typing, inadvertently revealing root passwords for election servers.

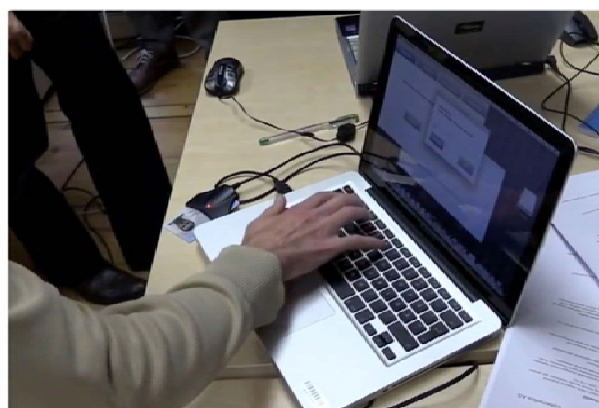


Figure 8: **Video shows national ID PINs** — During pre-election setup, someone types the secret PINs for their national ID card in full view of the official video camera.

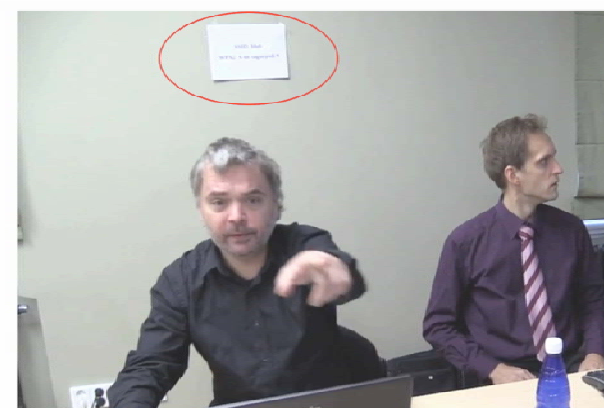


Figure 9: **Posted Wi-Fi credentials** — The official video of the pre-election process reveals credentials for the election officials' Wi-Fi network, which are posted on the wall.

Brief History of Swiss Voting Channels

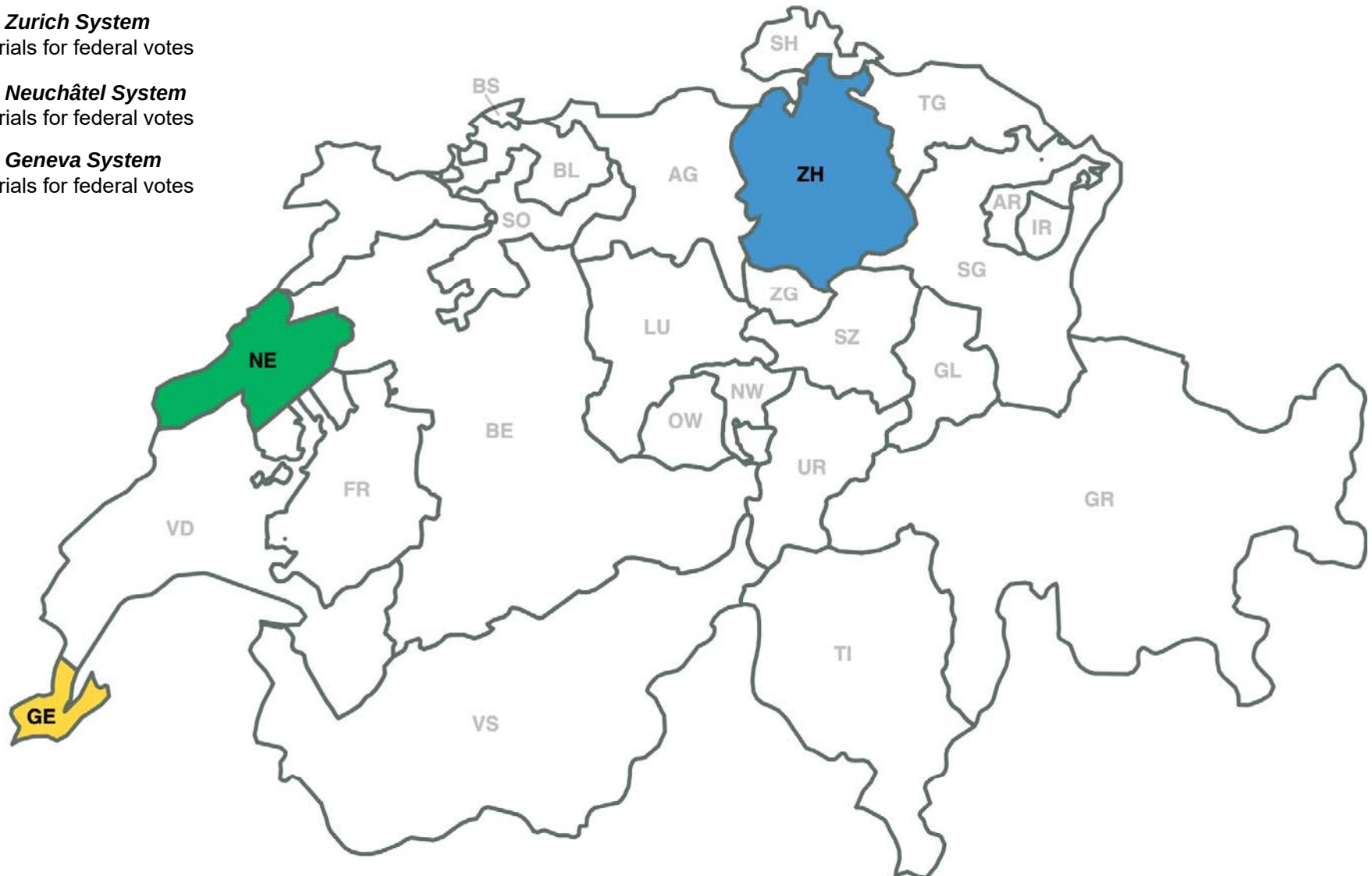
- ❑ A tradition of direct democracy (Landsgemeinde)
 - Introduction of “Remote Postal Voting” in the 1970’s which was generalized in the 1990’s
 - 1998: the Federal Council proposes to study Internet Voting (I-Voting) and by the year 2000, official start of the Vote “électronique” project with three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



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

First Trials, Initial Pilot Phase

-  **2004 Zurich System**
first trials for federal votes
-  **2005 Neuchâtel System**
first trials for federal votes
-  **2004 Geneva System**
first trials for federal votes

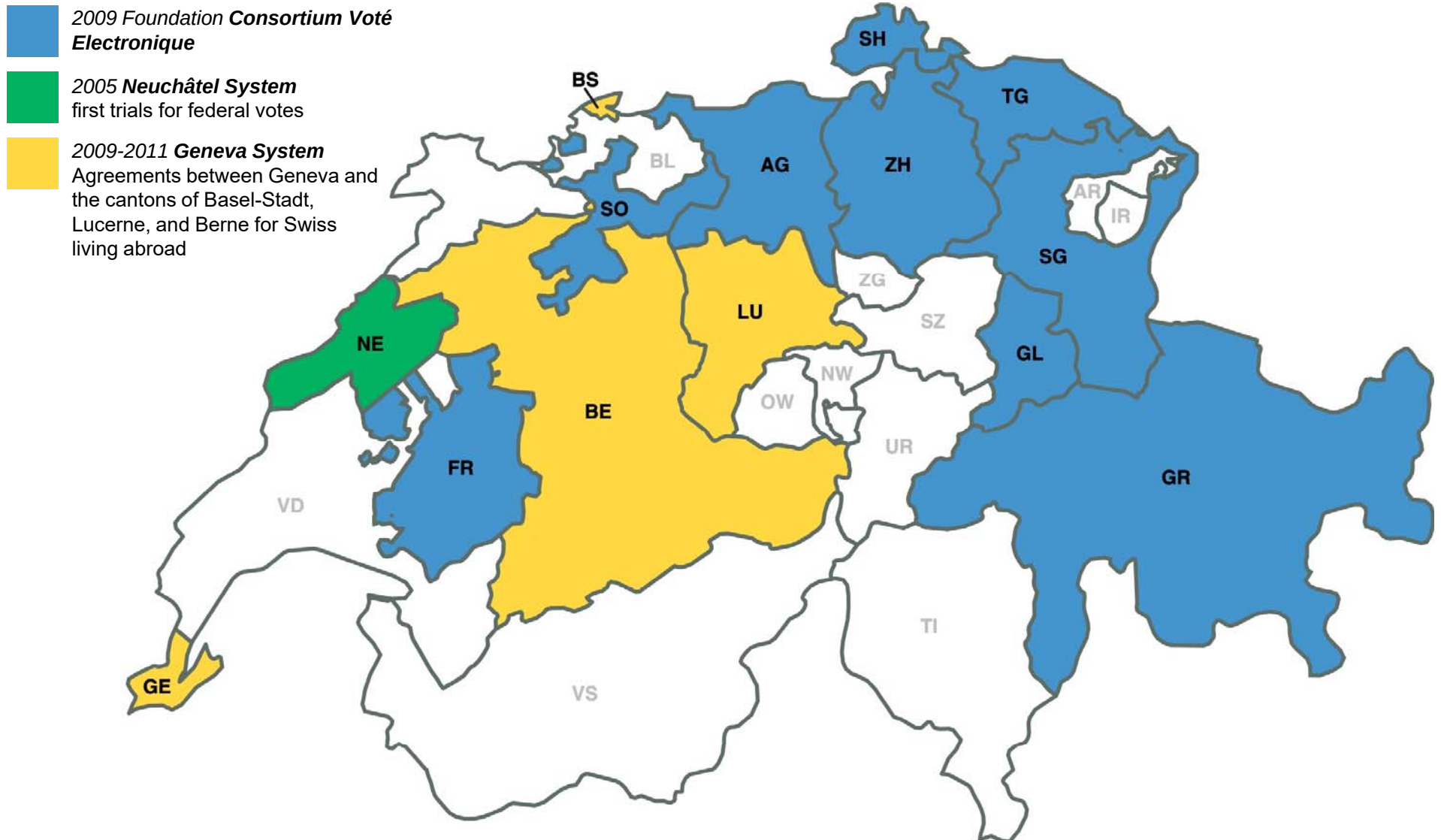


Extension of Trials

- ❑ In 2006, the Federal Government opened the door for all cantons to use *limited* internet voting:
 - 20% of the cantonal electorate (later extended to 30%);
 - 10% of the federal electorate

- ❑ Geneva and Zurich (Vote Consortium) started offering their system to other cantons
 - Some drawbacks were also experienced:
 - Regulatory issues in Geneva (2005 – 2007)
 - Technical issues in Zurich (2011 – now)

Extension of Swiss-wide Pilots



Situation as of 2011

■ Geneva System

- Canton owns the SW and operates the system
- Developed by Geneva IT Department
- Voting Protocol by Bern University of Applied Sciences

■ Zürich / Vote Électronique Consortium System

- Canton owns the SW, external company (Unisys) operates it
- Developed by Unisys

■ Neuchâtel System

- Canton owns the SW and operates the system
- Developed by ScytI
- Embedded in “Guichet unique”, as one of many offerings

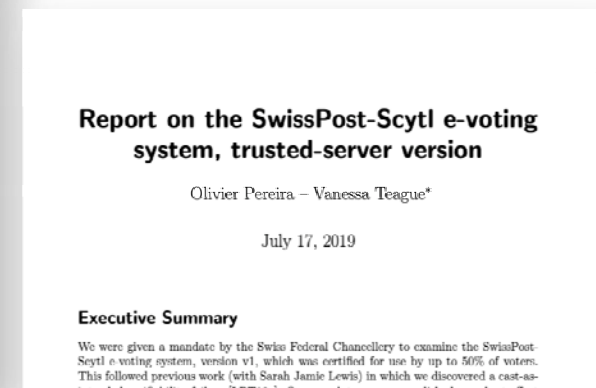
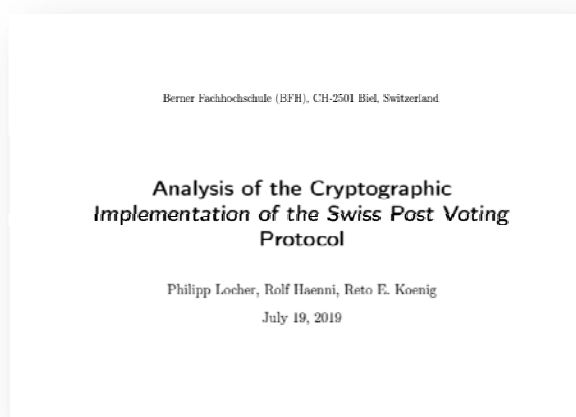
New Swiss Regulations in 2014 (VEleS)

- ❑ In 2013 new regulations regarding REV in CH
 - Federal Chancellery Ordinance on Electronic Voting
«161.116 - Verordnung der BK über die elektronische Stimmabgabe vom 13. Dezember 2013 (VEleS)»
- ❑ Framework for authorization of voting systems with three different levels, linked to the amount of allowed electorate

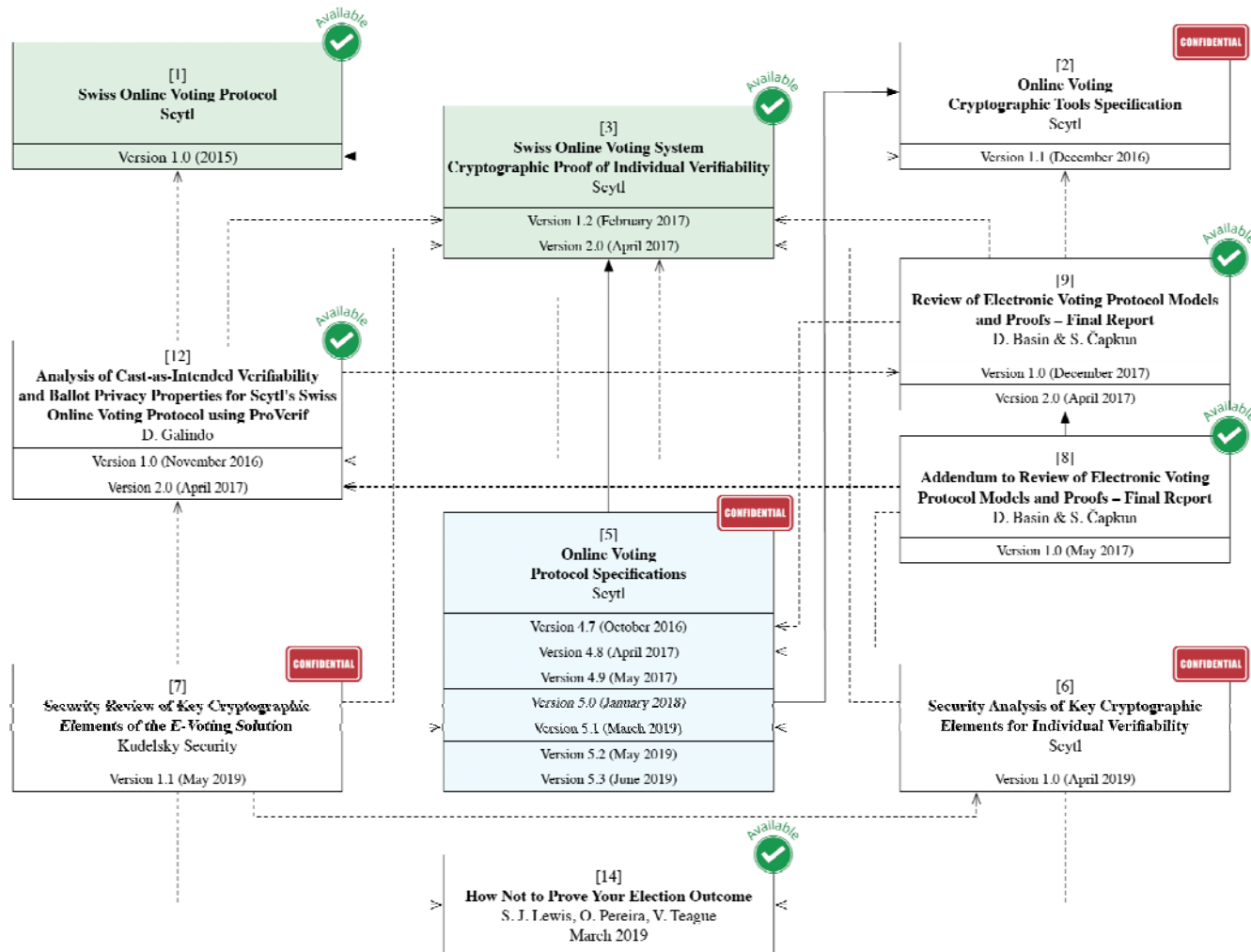
Level	Limit ⁽¹⁾	Requirements	Certification
1	30% cantonal 10% Swiss	Functional and security • BSI Common Criteria PP for Internet Voting Products • Council of Europe standards	• None, only ChF experts revisions of documentation (risk assessment, security architecture...) and security tests of system (functional and infrastructure)
2	50% cantonal 30% Swiss	Individual verifiability • Cast-as-intended verifiability • Recorded-as-cast verifiability	• Security: Common Criteria EAL 2 • Cryptography: Security and formal proofs (printing, server and tally are trusted) • Infrastructure and printing offices
3	No limit	Complete verifiability • Individual verifiability • Counted-as-recorded verifiability • Control components (2 or 4)	• Security: Common Criteria EAL 2 + EAL 4 (control components) • Cryptography: Security and formal proofs (printing and one control component are trusted) • Infrastructure and printing offices

Publication of Source Code 2019

- ❑ Publication of the source code in February 2019, researchers have uncovered significant security flaws in the new, fully verifiable, system provided by Swiss Post (sVote, developed by ScytI)
 - One of the security issues relates to individual verifiability and thus to the system already used. As a result, the system was not available May 2019.



sVote Dependencies



Advertisement on Public Initiative



Eidgenössische Volksinitiative

«Für eine sichere und vertrauenswürdige Demokratie»



Swiss public initiative on a "Secure and trusted democracy"

Proposed Law

Eidgenössische Volksinitiative «Für eine sichere und vertrauenswürdige Demokratie (E-Voting-Moratorium)»

Art. 197 Ziff. 12^[2]

12. Übergangsbestimmung zu Art. 39 Abs. 1^{bis} (Verwendung elektronischer Verfahren zur Stimmabgabe)

¹ Artikel 39 Absatz 1^{bis} tritt mit der Annahme durch Volk und Stände in Kraft; mit der Annahme sind sämtliche Bestimmungen des kantonalen Rechts und des Bundesrechts über elektronische Verfahren zur Stimmabgabe nicht mehr anwendbar.

² Die Bundesversammlung kann das Verbot durch Bundesgesetz aufheben, wenn gewährleistet ist, dass mindestens die gleiche Sicherheit gegen

Manipulationshandlungen wie bei der handschriftlichen Stimmabgabe besteht,
namentlich wenn unter Wahrung des Stimmgeheimnisses:

*... if it is guaranteed that **at least the same security against manipulation exists as in the case of hand-written voting** ...*

Comparing “Systems”

RPV ? REV



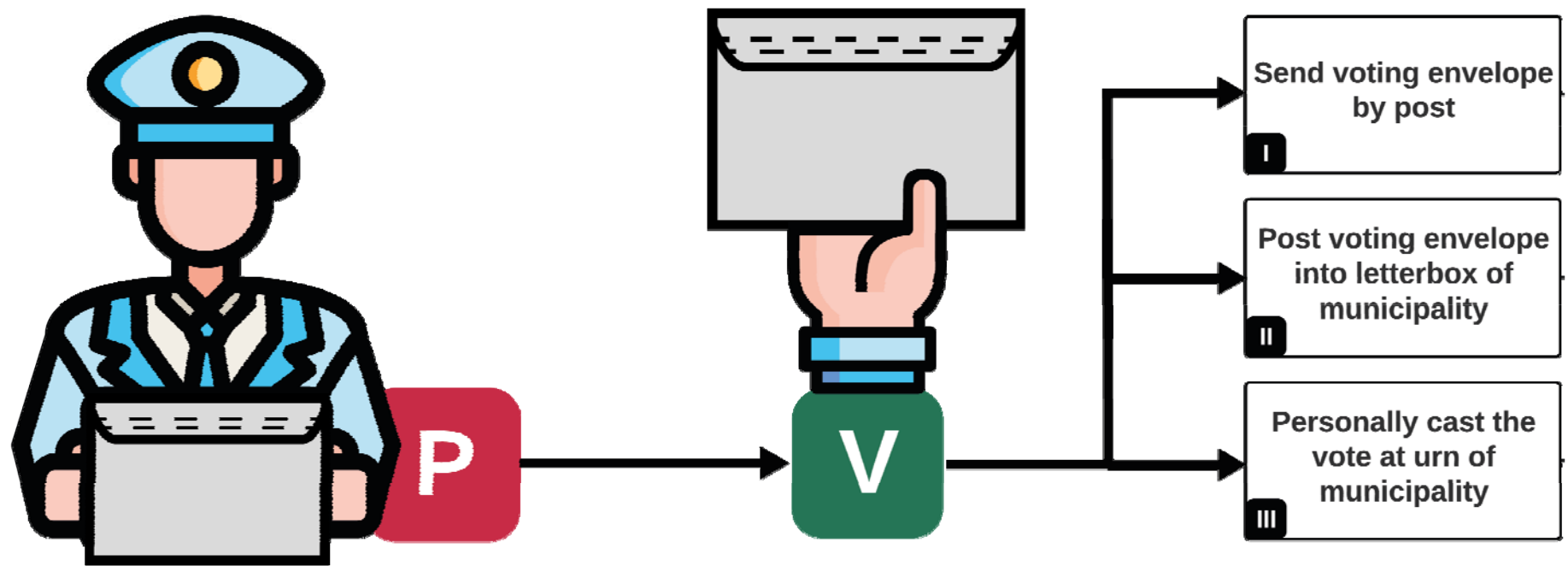
The Swiss RPV Case

- ❑ 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

[KS19] C. Killer, B. Stiller: The Swiss Postal Voting Process and Its System and Security Analysis, E-VOTE-ID 2019

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

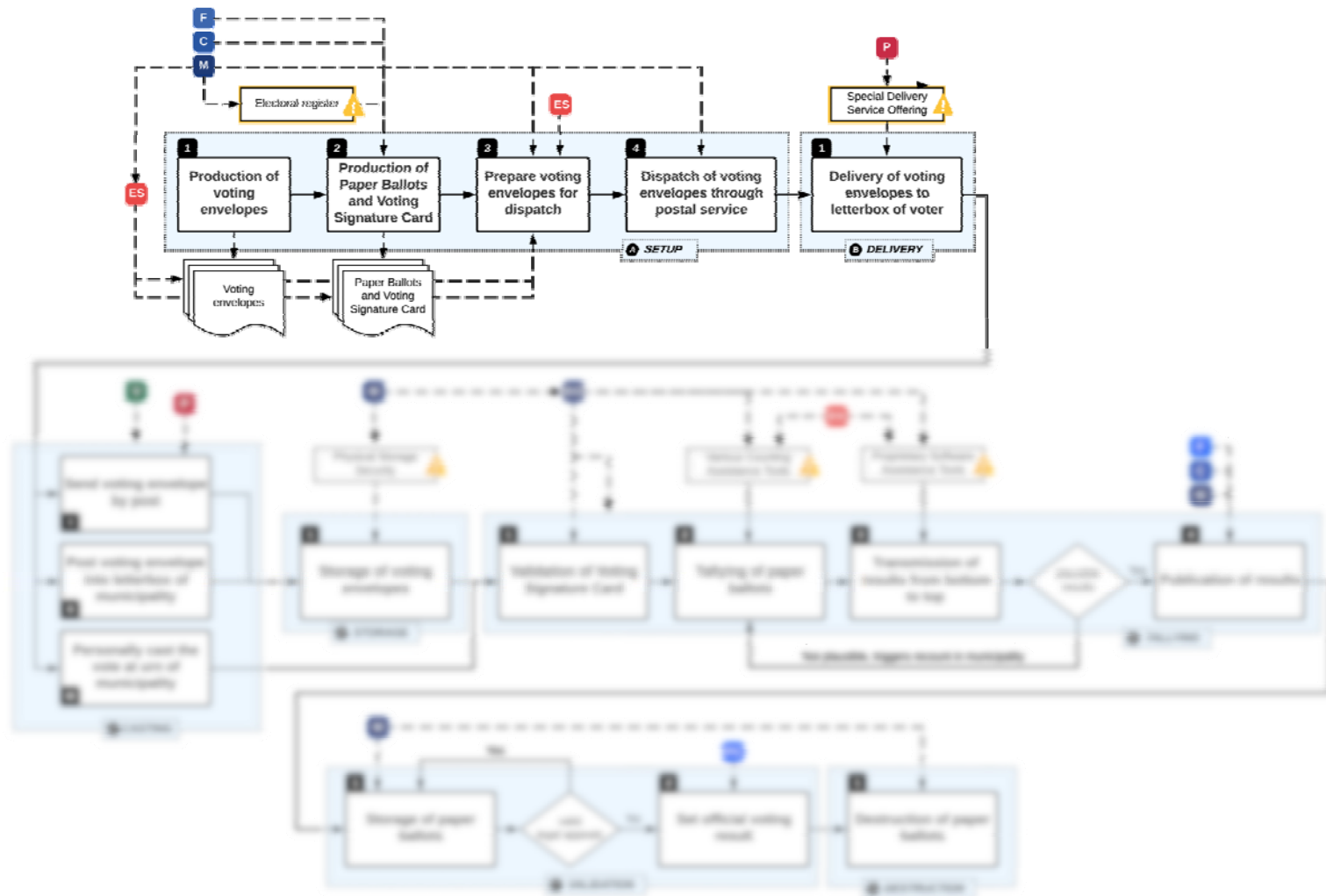
- Divided into phases A to G with various stakeholders

- 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

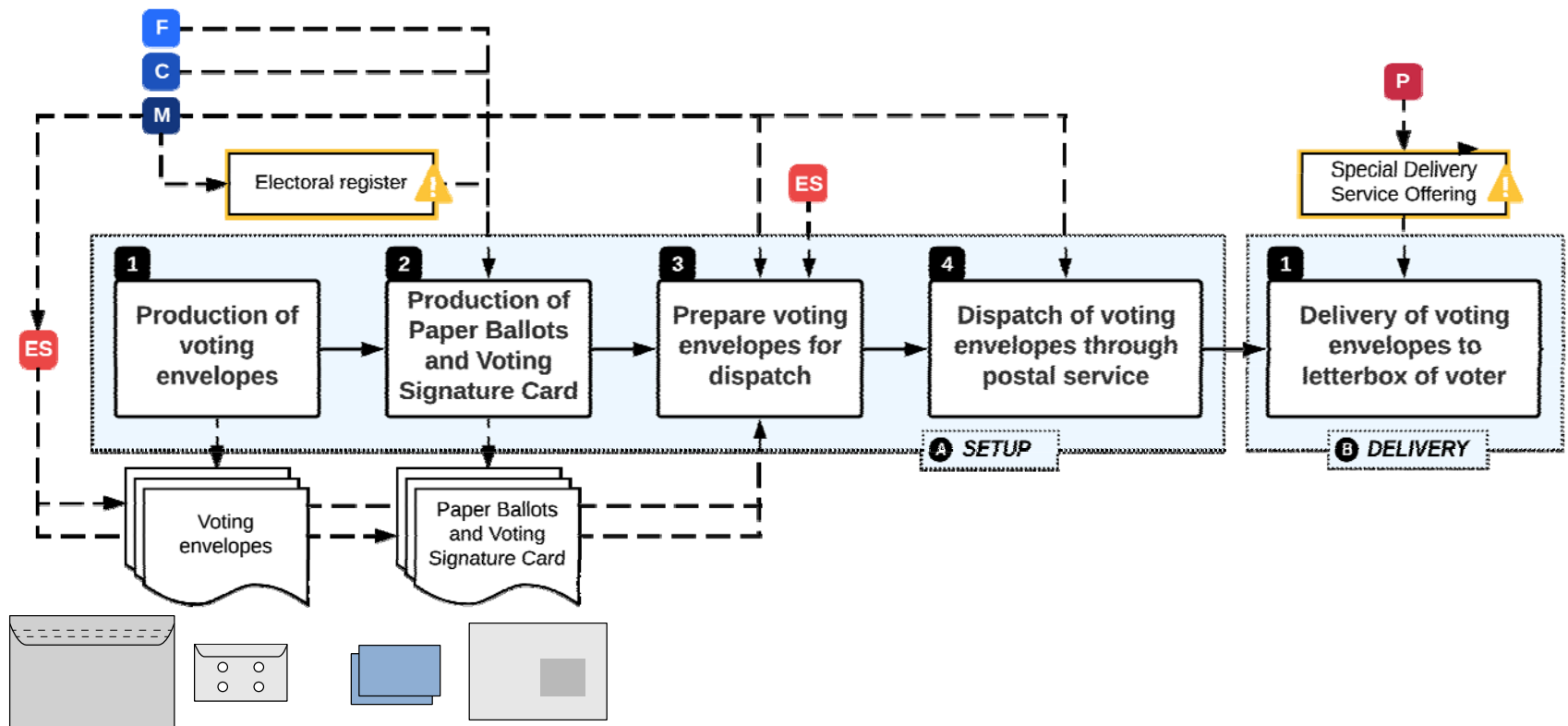
PVPF in Detail



[KS19]

PVPF: Postal Voting Process Flow

A: Setup, B: Delivery



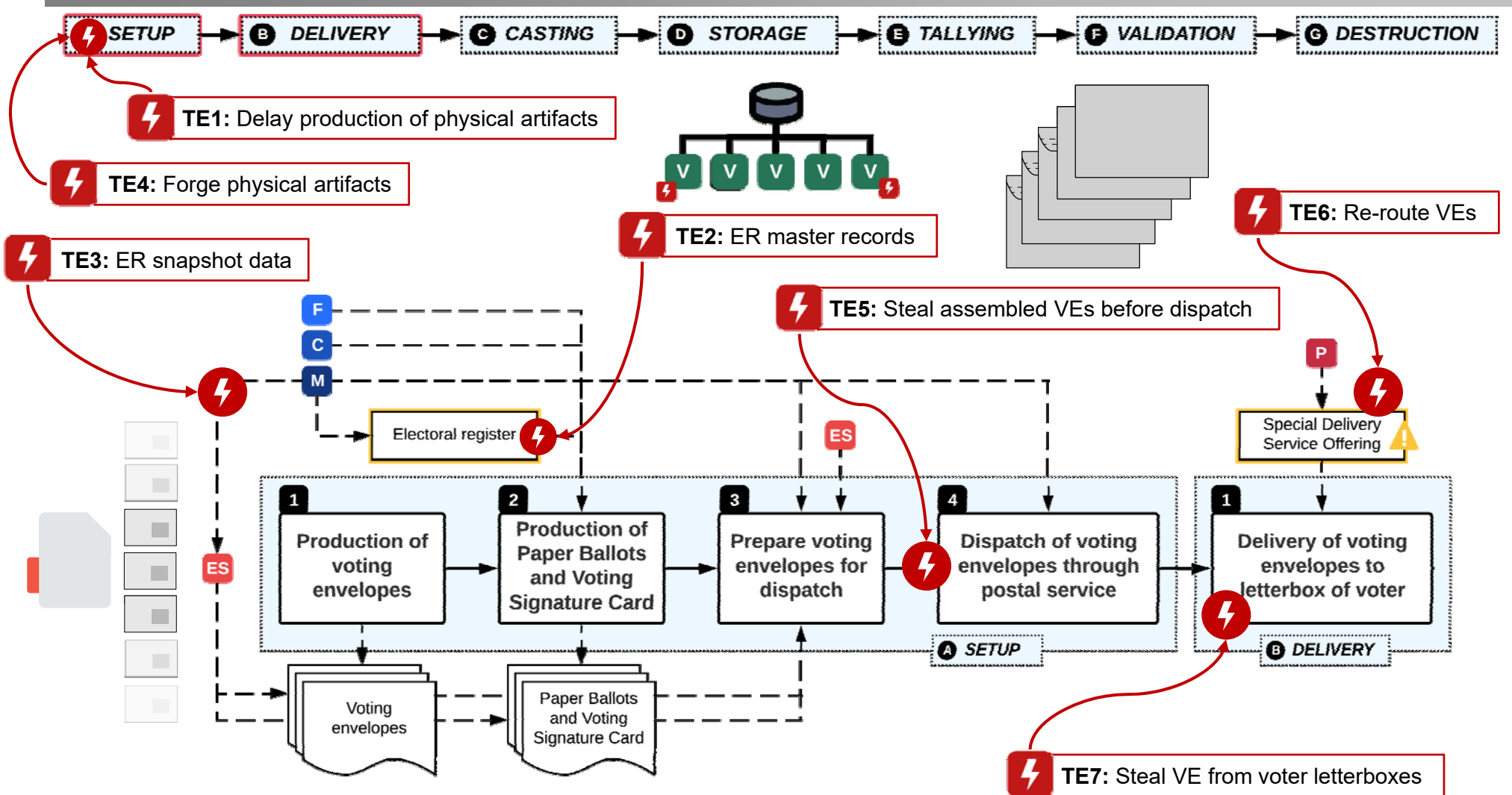
F	Federal Government	C	Cantonal Government	EO	Municipal Election Office	P	The Swiss Post
FC	Federal Chancellery of Switzerland	M	Municipality	V	Eligible Voter	ES	External Supplier
						!	Security Threat

[KS19]

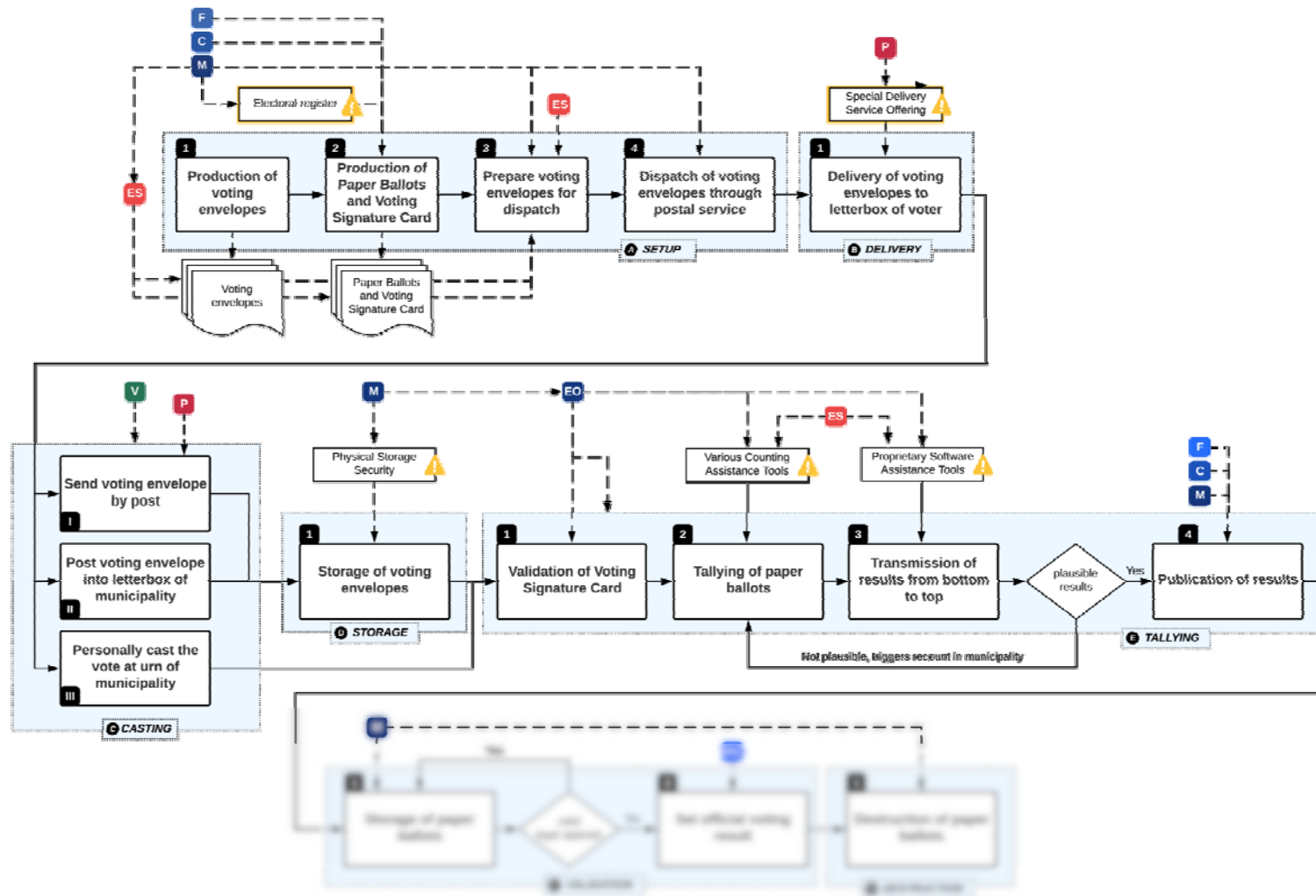
A: Setup, B: Delivery



THREAT EVENTS

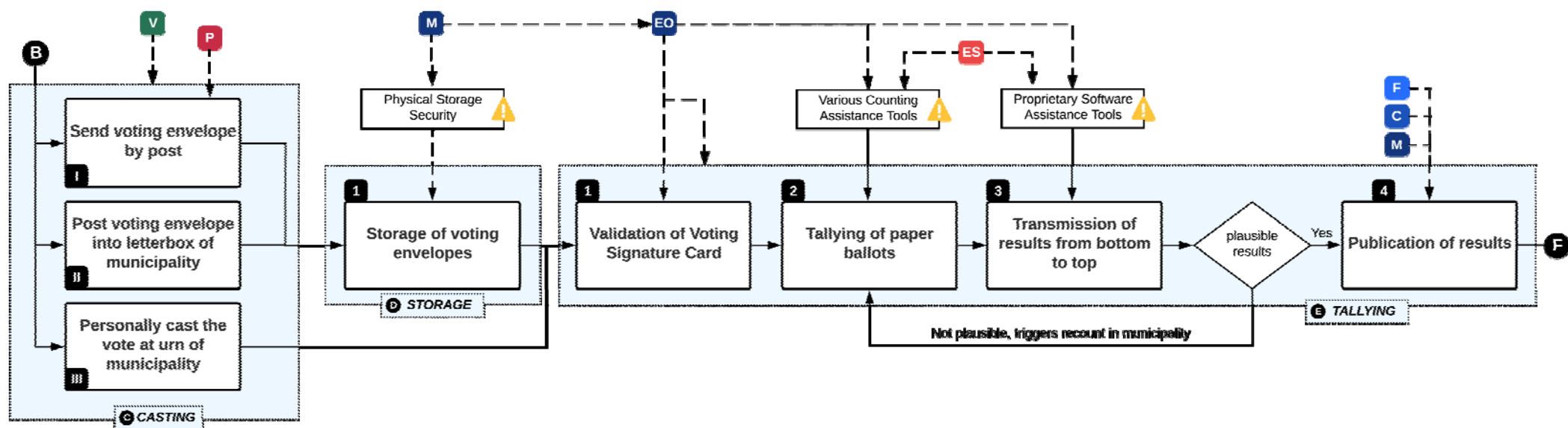


PVPF in Detail



PVPF: Postal Voting Process Flow

C: Casting, D: Storage, E: Tallying

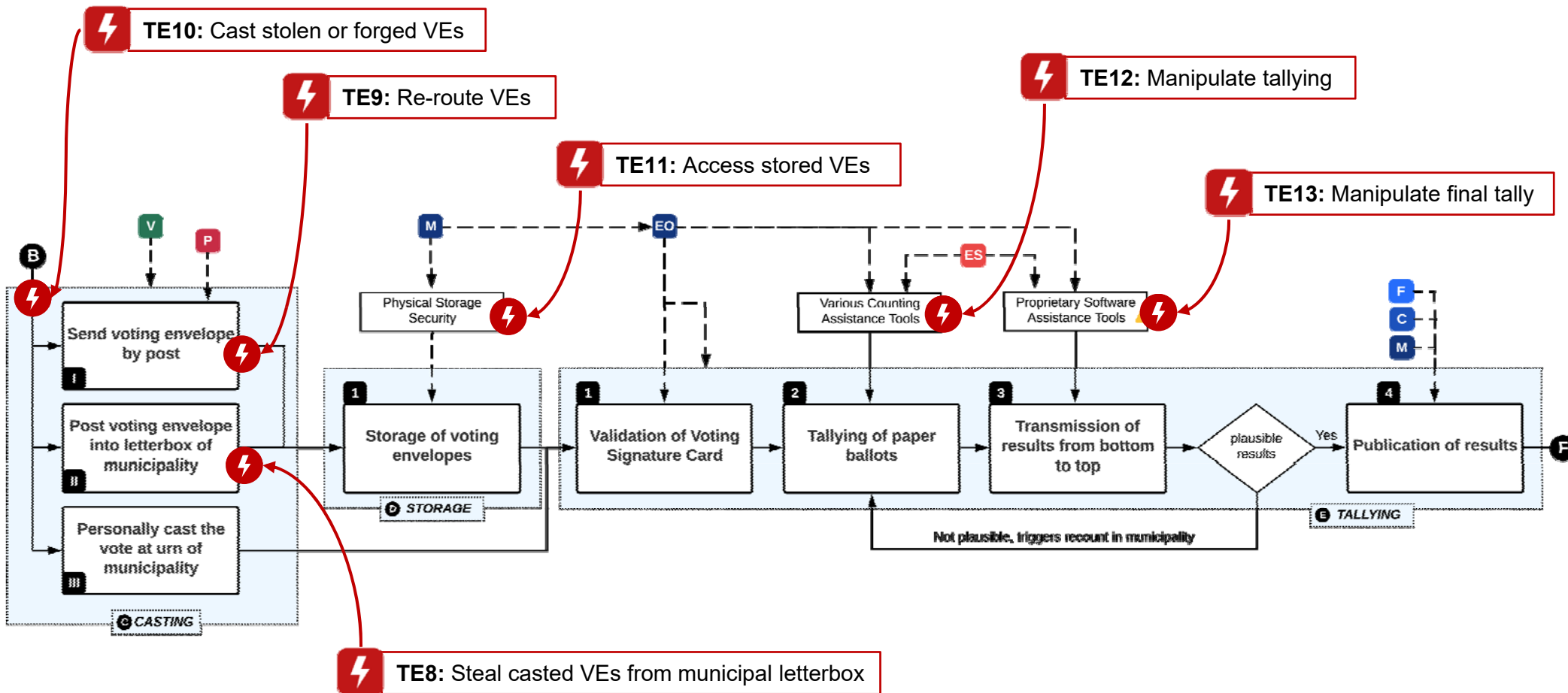


F	Federal Government	C	Cantonal Government	EO	Municipal Election Office	P	The Swiss Post
FC	Federal Chancellery of Switzerland	M	Municipality	V	Eligible Voter	ES	External Supplier
						!	Security Threat

C: Casting, D: Storage, E: Tallying



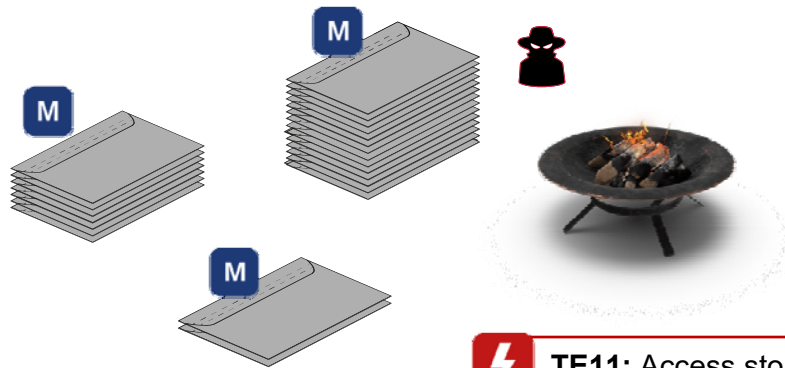
THREAT EVENTS



C: Casting, D: Storage, E: Tallying



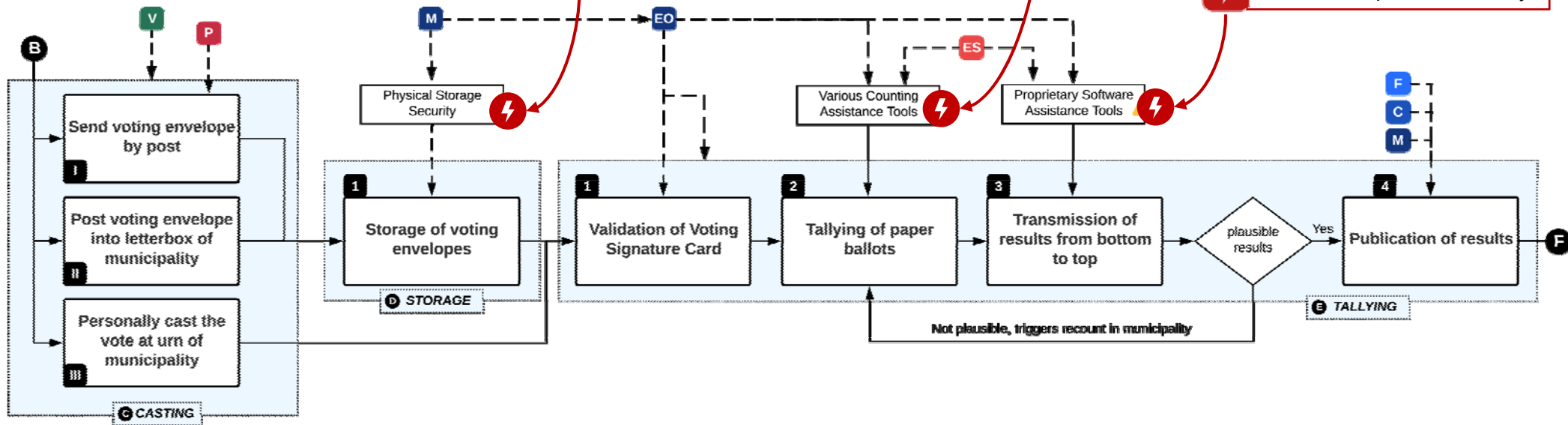
THREAT EVENTS



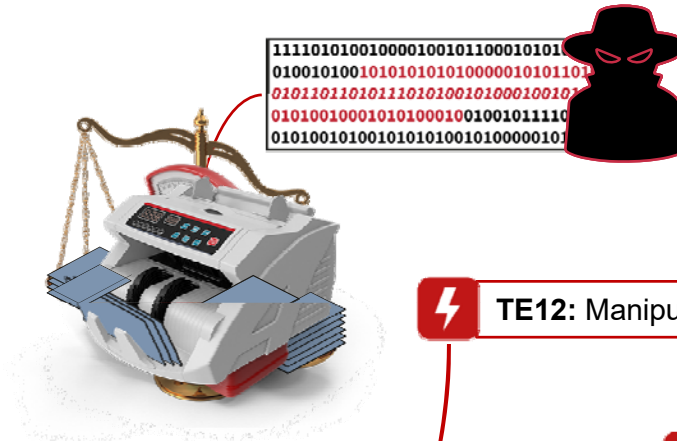
⚡ TE11: Access stored VEs

⚡ TE12: Manipulate tallying

⚡ TE13: Manipulate final tally

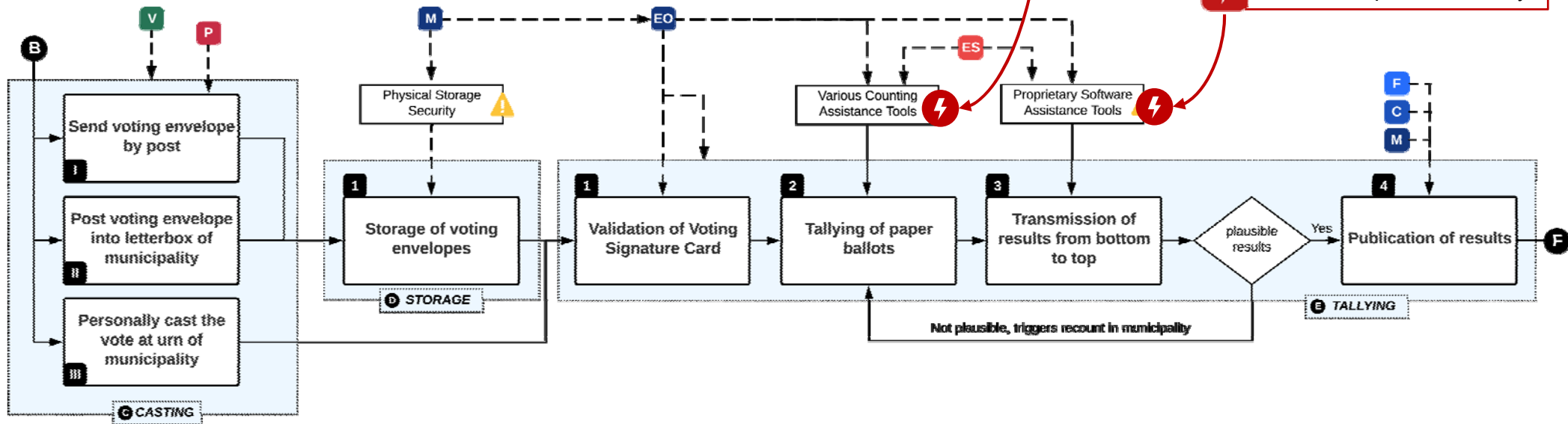


C: Casting, D: Storage, E: Tallying THREAT EVENTS



 **TE12: Manipulate tallying**

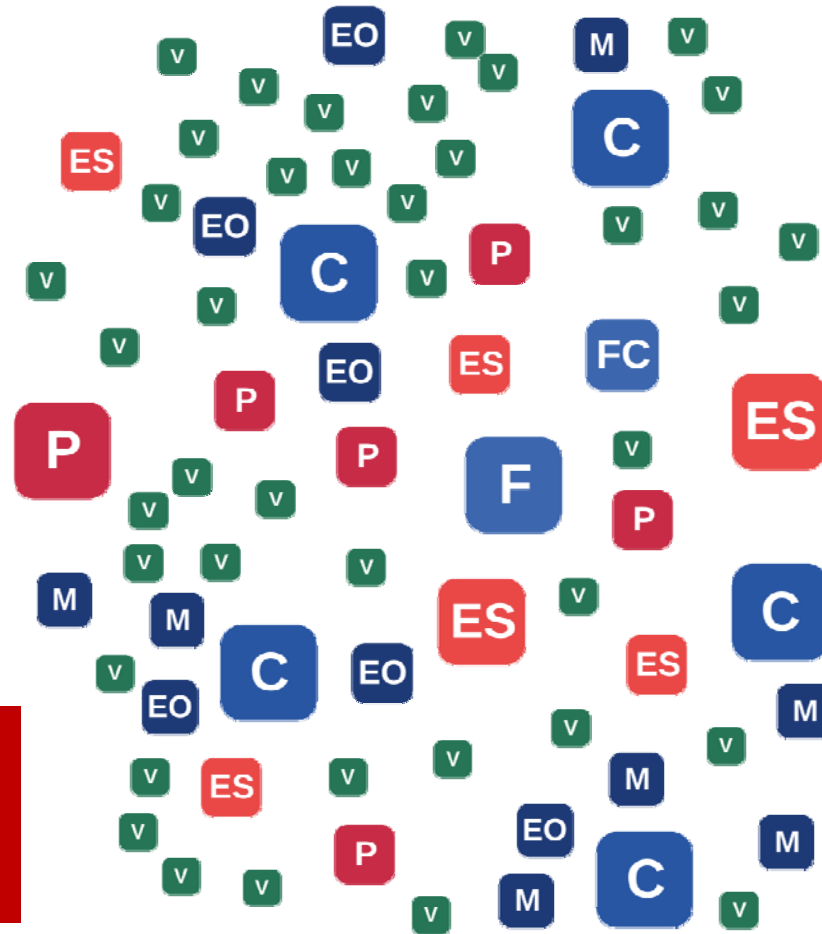
 **TE13: Manipulate final tally**



Conclusions on the Swiss RPV

**Heterogeneous
Processes**

**Substantial
Trust in Third
Parties**



**Distribution of
Trust and Physical
Decentralization**

Theoretical Properties

REV Requirements

□ Privacy

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

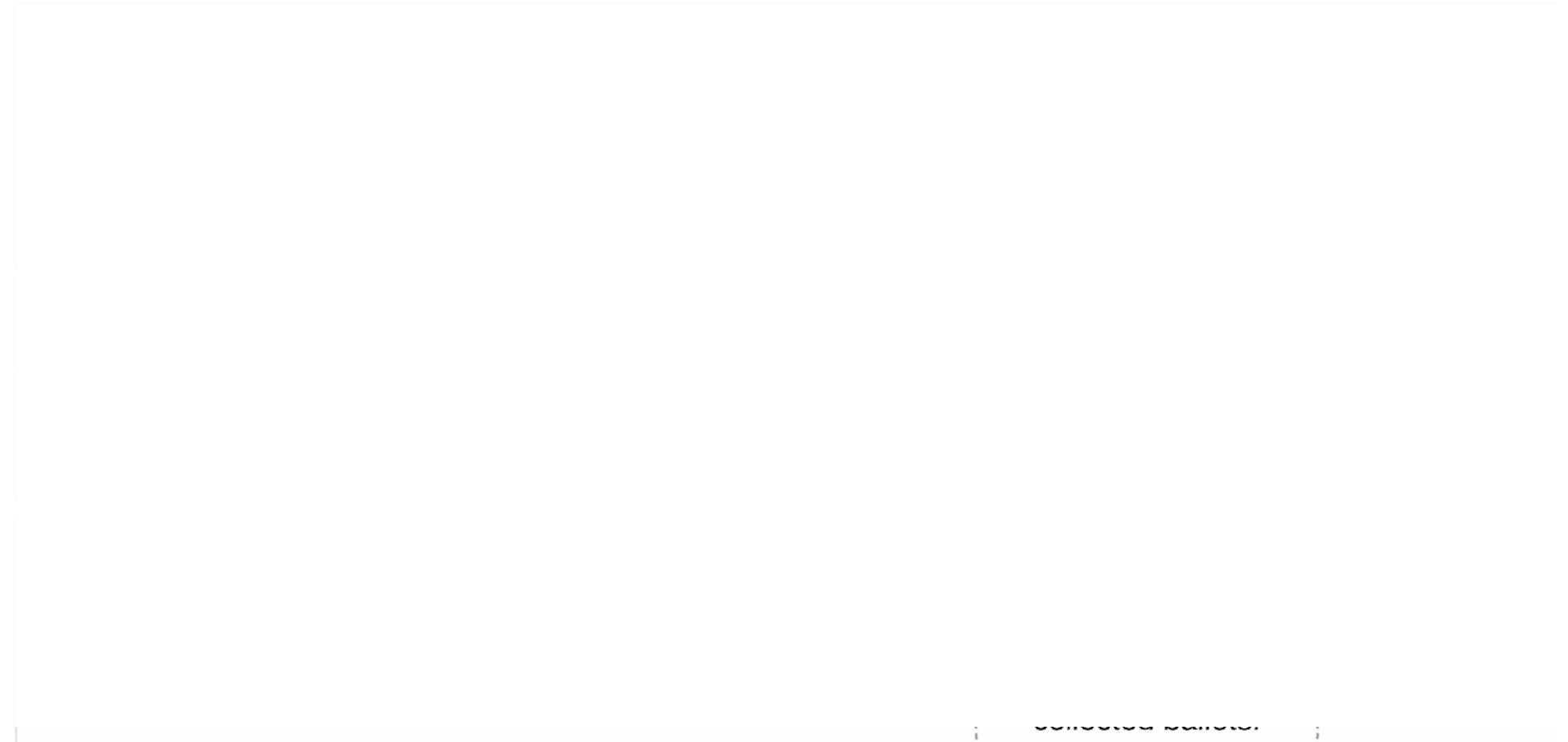
□ Verifiability

- 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

A voter cannot

nst:
ed abstention,
ed randomised voting
ed to give up voter
ential

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
 - ❑ Tallied As Recorded
 - The Voter’s ballot counts as received

Fairness and Unforgeability

❑ Fairness

- concerns the impossibility to deduct a partial tally, *before the end of the vote casting period*.
- REV schemes should not allow for intermediate results, which potentially influence voters that have not voted yet.

❑ Eligibility Verifiability

- anyone can check that each vote in the election outcome was cast by a registered voter and there is at most one vote per voter

❑ Unforgeability

- Only eligible voters can construct authorised ballots.

Software Independence

- ❑ Software Independence

- A voting system is software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome

- ❑ Addresses the difficulty of verifying

- Complex software in a completely electronic voting systems

- ❑ Problem: providing assurance that the voting software is in fact correct

- Verify the election results, not the voting system

Refinements of Software Independence

- ❑ Weak Software Independence
 - A voting system that is ***weakly*** software-independent conforms to the basic definition of software-independence, that is, ***there is no recovery mechanism***

- ❑ Strong Software Independence
 - A voting system is ***strongly*** software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome, and moreover, a detected change or error in an election outcome (due to change or error in the software) can be corrected without re-running the election

REV Building Blocks (1)

- ❑ Secret-Ballot Voting Schemes, *i.e.*, *voting protocols* describing the *process*
- ❑ Cryptographic Primitives, *i.e.*, *procedures* used in the *protocols* to assure privacy and verifiability
- ❑ Public Bulletin Board (PBB), *i.e.*, *ballot box* saving all results and logs of the *procedures*, making the process verifiable

Building Blocks for REV Schemes

Secret Ballot Voting Schemes

scheme	privacy	verifiability	attacks	based on	
FOO92 [32]	BP	UV	KR05 [44]	BS	BP: Ballot Privacy RF: Receipt-Freeness CR: Coercion-Resistance EBP: Everlasting Ballot-Privacy
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	BS: Blind Signatures HE: Homomorphic Encryption MC: Multiparty Computation MN: Mixnet CS: Commitment Scheme
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	Based on „Privacy and Verifiability in Voting Systems” by H. Jonker 2013
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	

Homomorphic Encryption

□ Homomorphic Encryption (HE)

$$enc_k(m_1) \otimes enc_k(m_2) = enc_k(m_1 \oplus m_2)$$

- $\otimes$ appropriate operation on ciphertext messages
- $\oplus$ appropriate operation on plaintext messages

- Allows two encrypted messages to be combined meaningfully (by using $\oplus$)
- The actual operations represented by $\otimes$ and $\oplus$ depend on the used cryptographic system.

Homomorphic Encryption

- ❑ 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

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

Proving Ciphertext Validity

- ❑ But how do we tackle the encryption malleability?
 - *i.e.* What happens if I encrypt 100 instead of 1?
 - We need a way to assure the validity of the ciphertext, while assuring Ballot Privacy

➤ ***Zero Knowledge Proofs!***

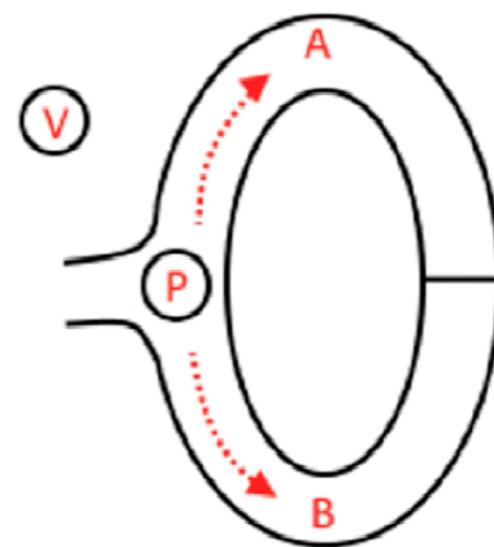
- Each voter proves that she cast a valid vote, without revealing her/his vote
- The authorities prove that they know their secret keys (that match the election public keys), without revealing their secret keys
- At the end of the election, the authorities prove that they have tallied correctly (decrypted the result correctly), again without revealing their secret keys

Zero Knowledge Proofs

- ❑ **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.*

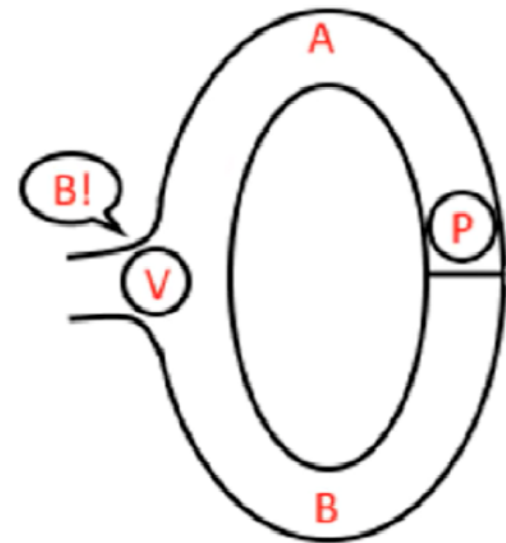
Ali Baba's Cave (1)

- ❑ 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** knows the password to open the hidden door **but does not want to reveal it**
- ❑ To prove to **Victor**, the verifier that Peggy knows the password, Peggy enters the cave and chooses a path



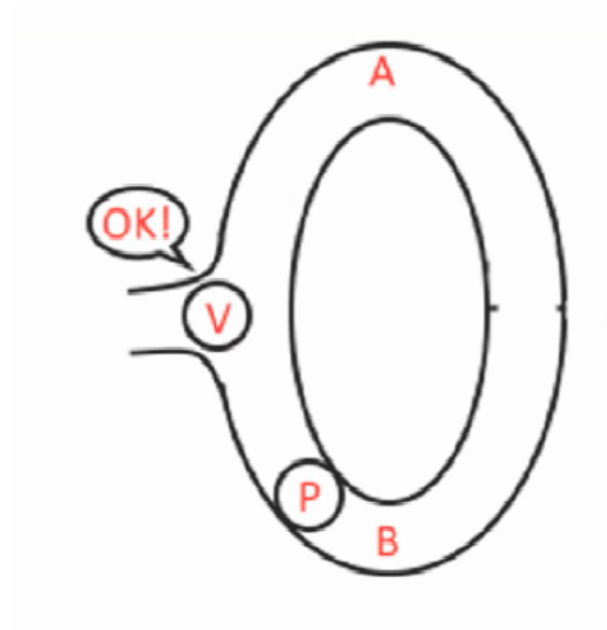
Ali Baba's Cave (2)

- ❑ 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 it to pass the test
 - On the other hand, would P had not known the password, he/she would have only had a 50% chance of returning from the demanded path

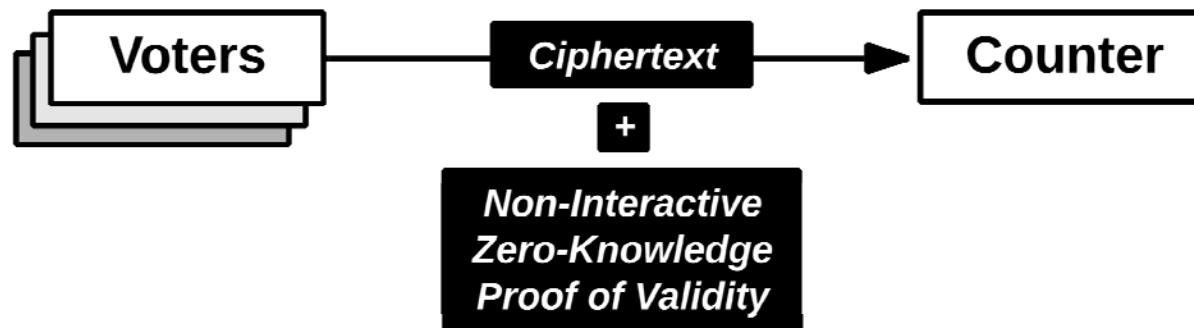


Ali Baba's Cave (3)

- ❑ Victor can challenge Peggy multiple times, thereby, decreasing the probability of Peggy being a fraudulent “prover” by a factor of two every time
 - 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



- ❑ 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

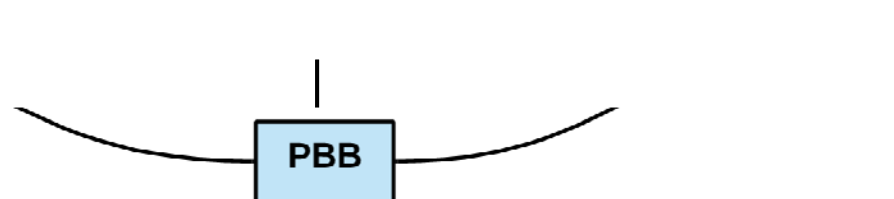
➤ *How can voters verify the election data?*

Public Bulletin Board (PBB)

- ❑ 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

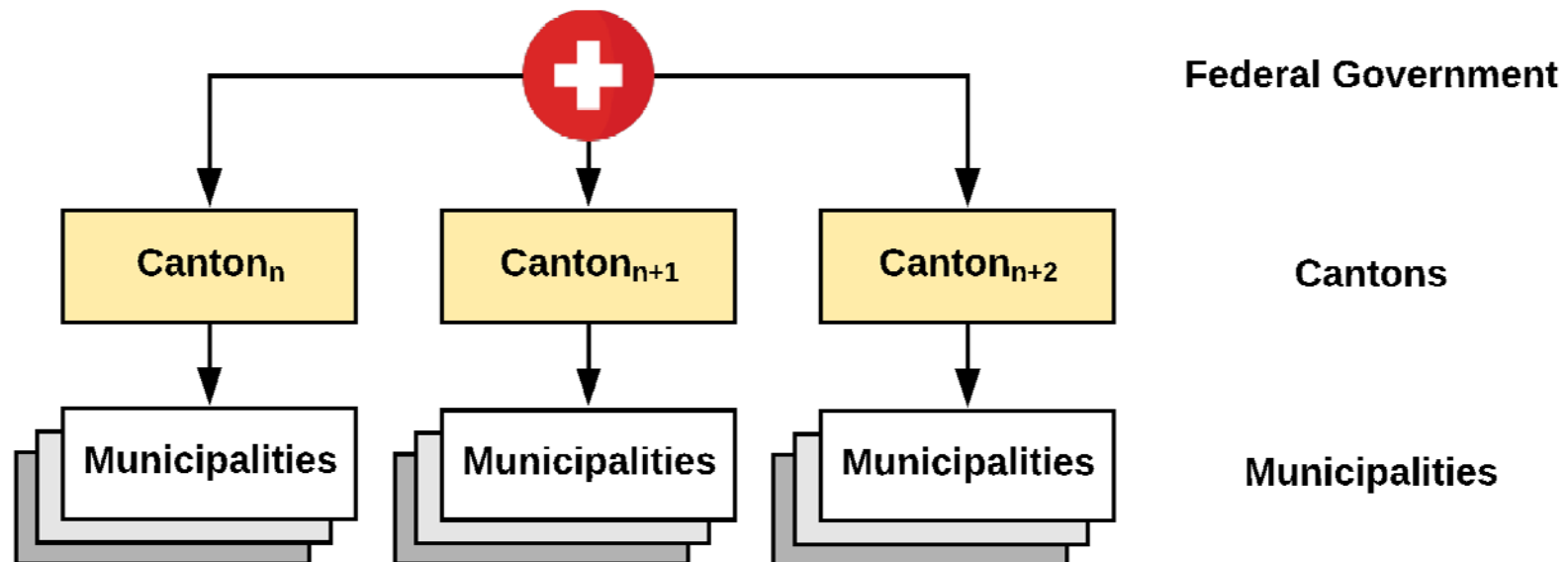
Public Permissioned Blockchain (BC)

- ❑ **Deployment** of a **Public Permissioned BC**
 - Read operations: **Public**
 - Write operations: **Permissioned**

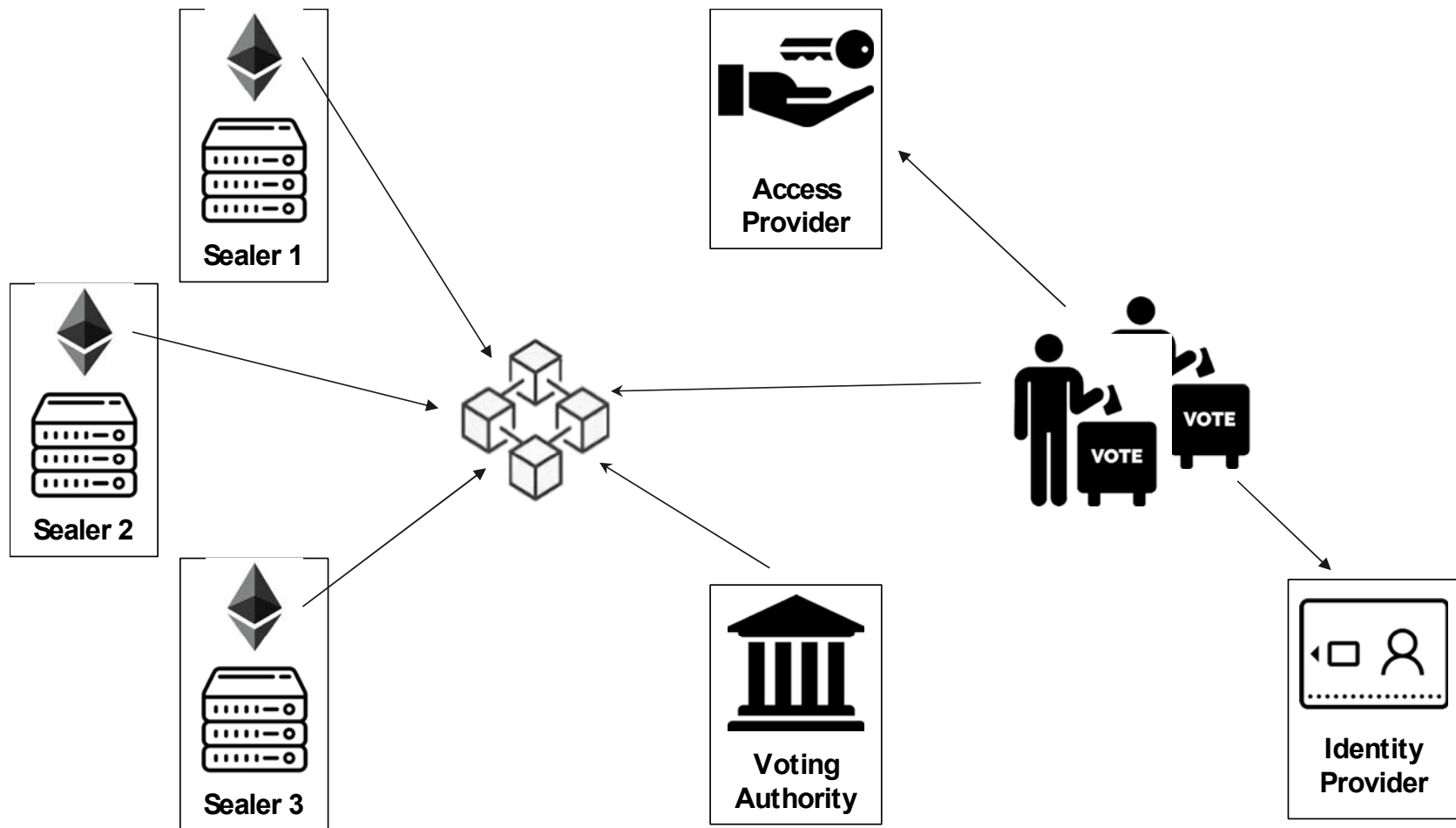


The Swiss Scenario

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



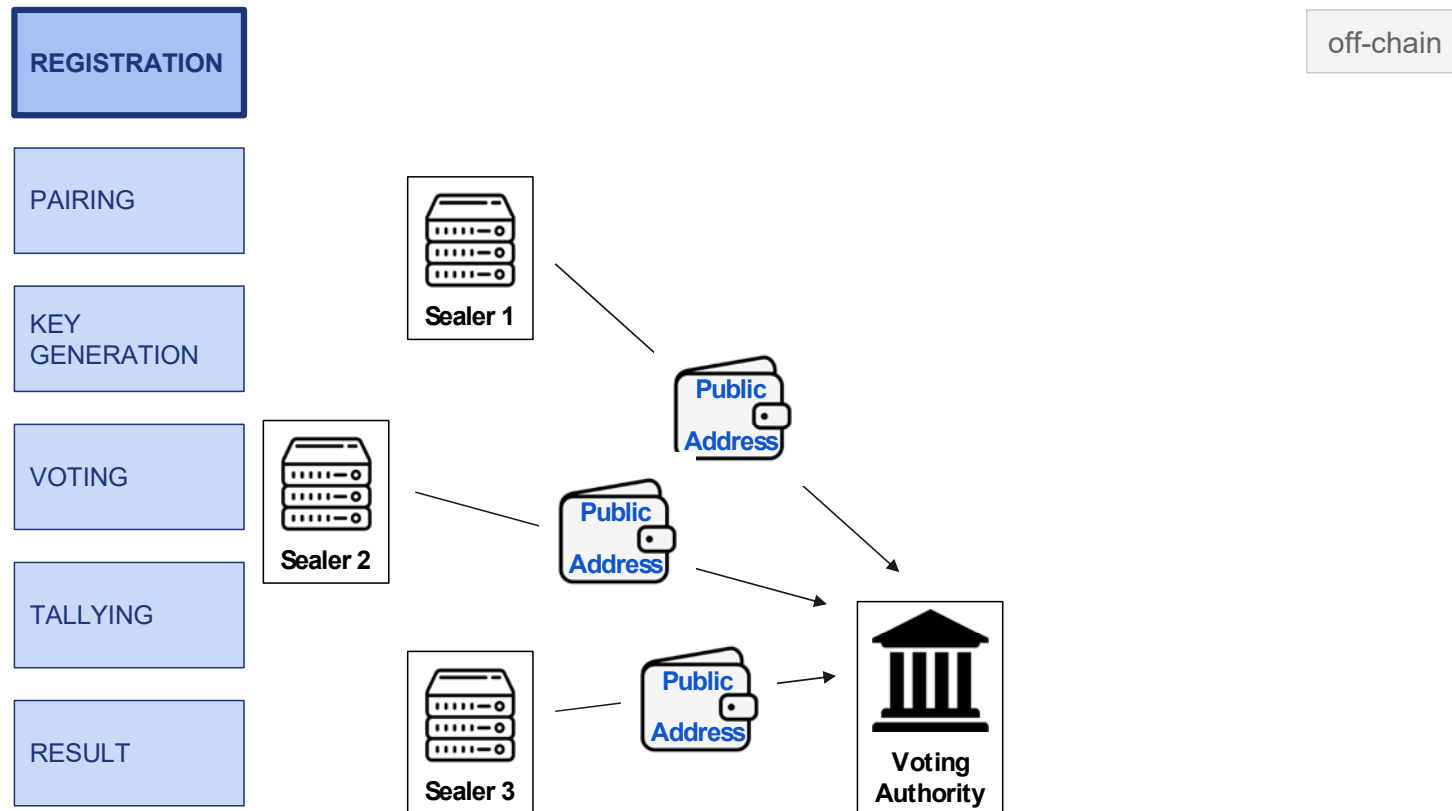
BC-based REV System: *Provotum*



Provotum 2.0 Identity Provisioning



Voting Protocol: Registration (1)



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 it's wallet address with the authority.

<->

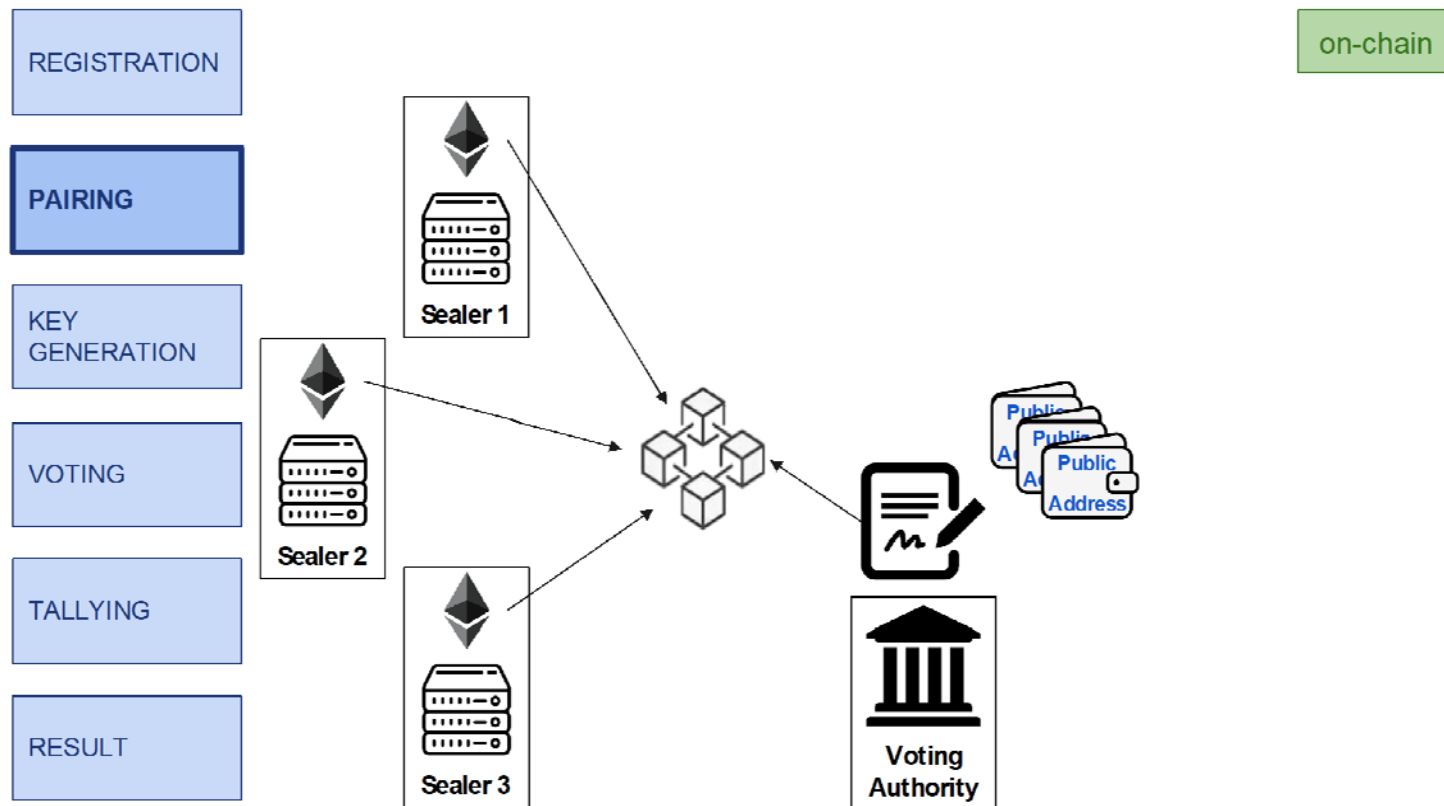
 currently 0/3 sealers are registered

please wait until all sealers have registered their address

NEXT STEP

Copyright © Nik Zaugg Alex Scheitlin Moritz Eck 2020.

Voting Protocol: Pairing (2)



Voting Protocol: Pairing (2)

Voting Authority

OFF CHAIN

✓ 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

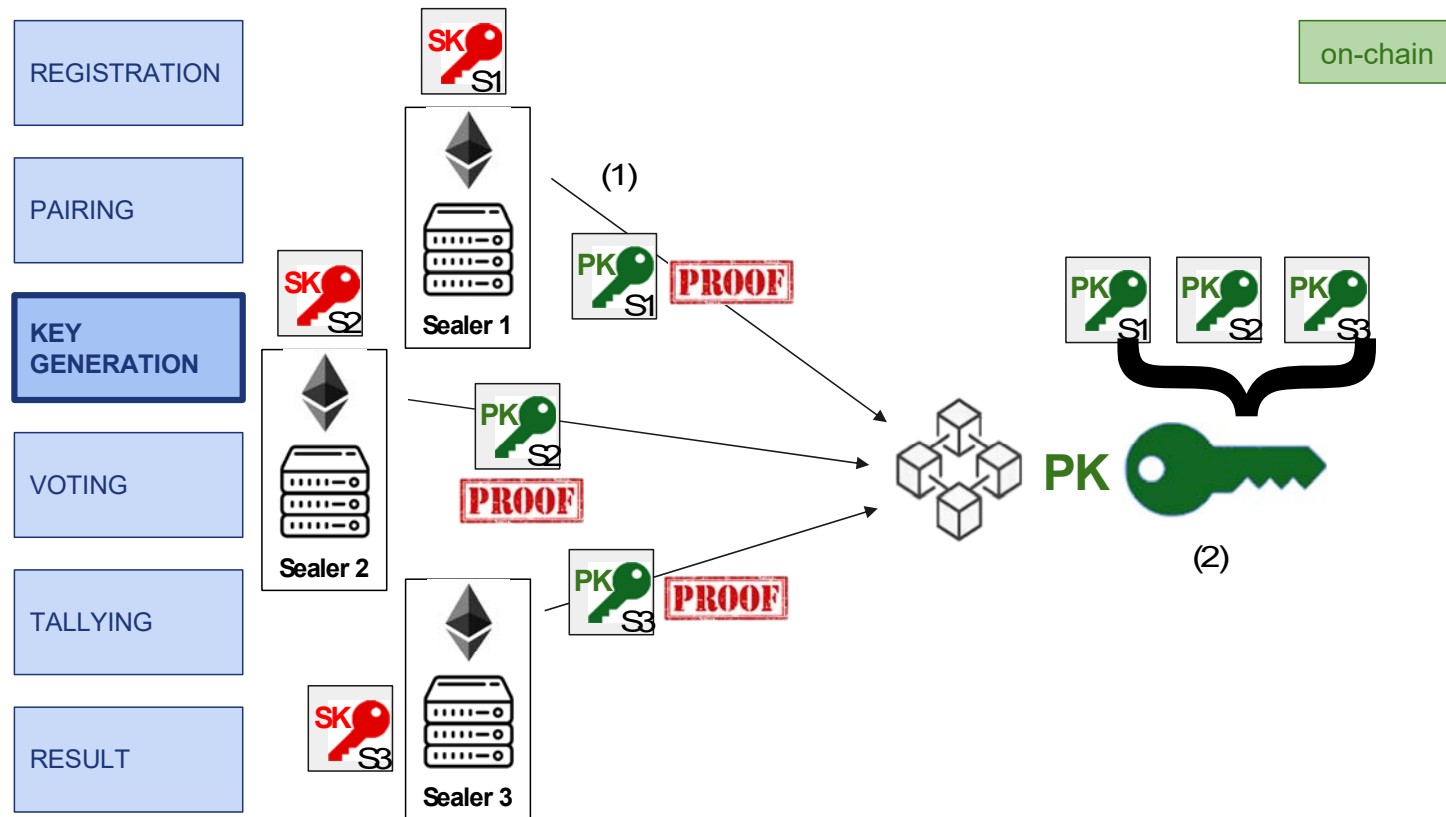
* please wait until all sealers have registered to deploy the contract

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

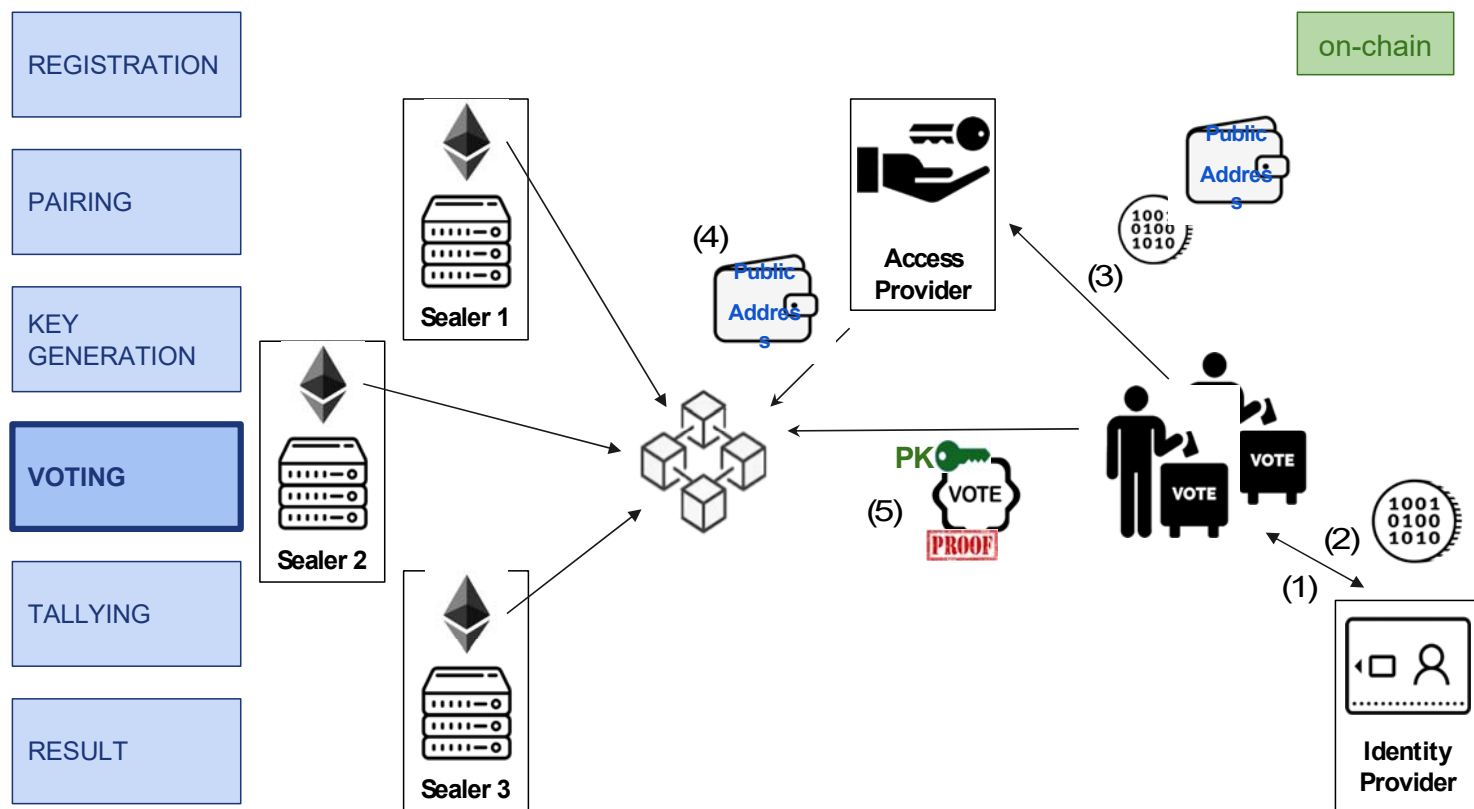
1

GENERATE PUBLIC KEY

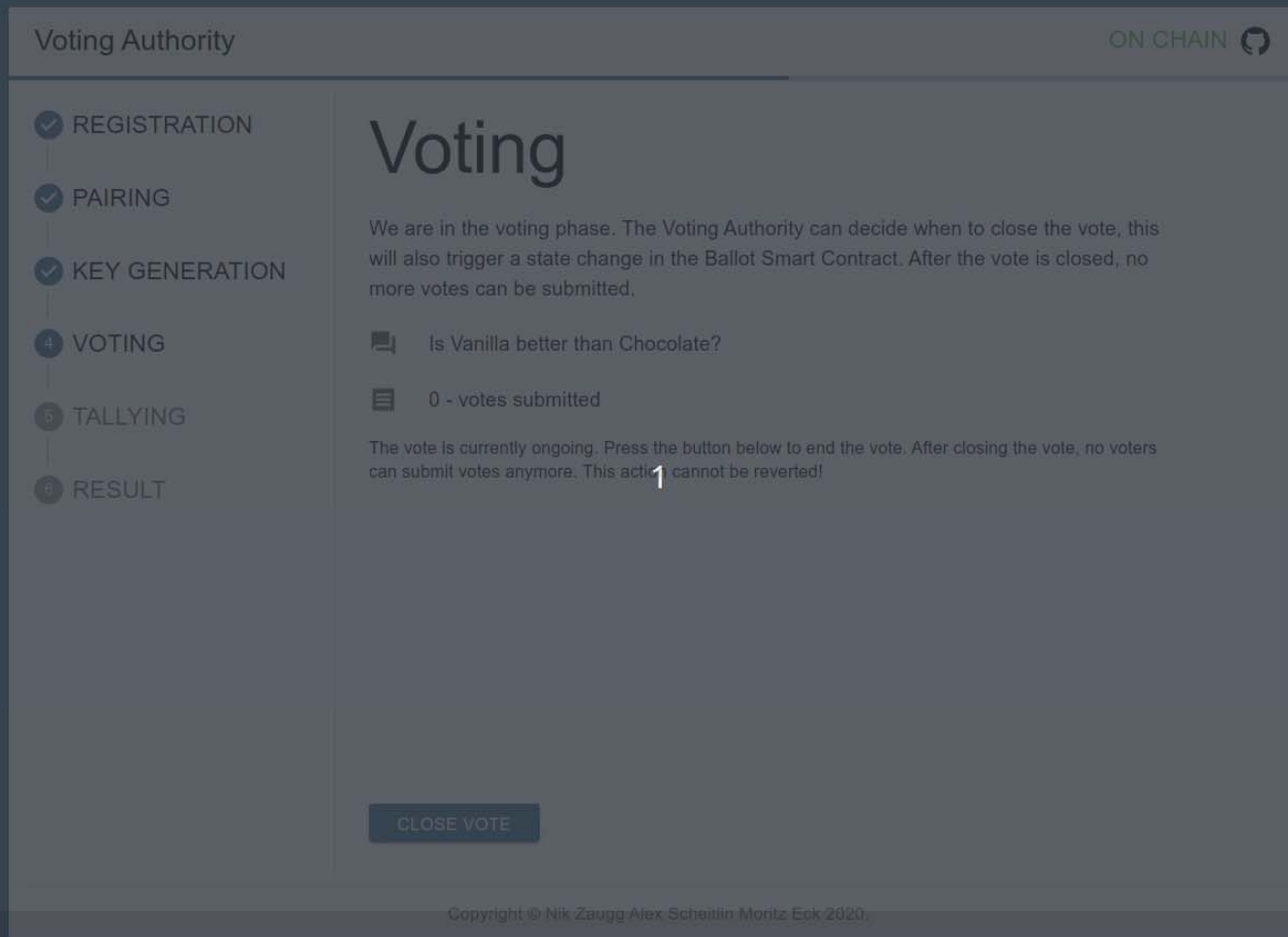
OPEN VOTE

Copyright © Nik Zaugg Alex Scheitlin Moritz Eck 2020.

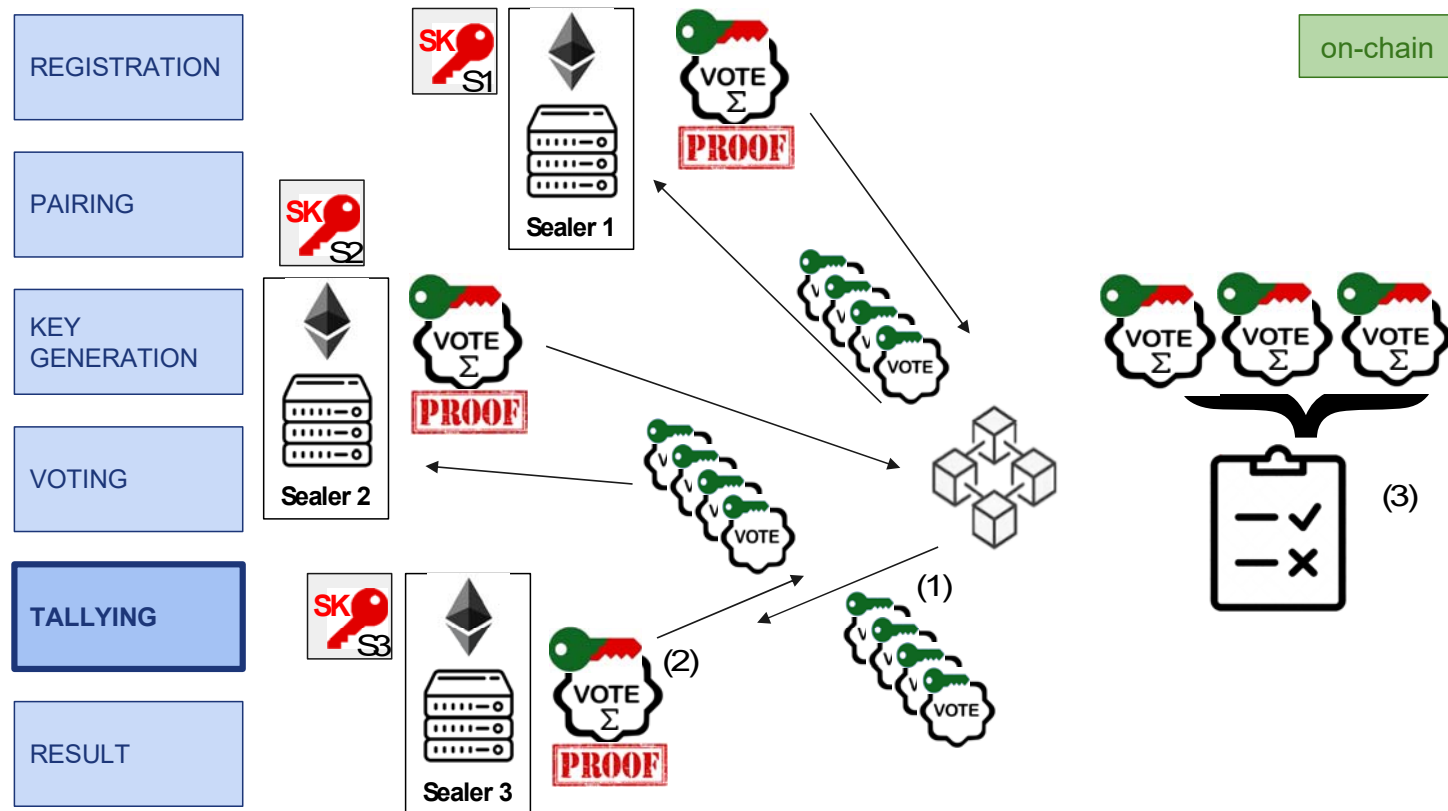
Voting Protocol: Voting (4)



Voting Protocol: Voting (4)



Voting Protocol: Tallying (5)



Voting Protocol: Tallying (5)

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.

1

GENERATE SUMMARY

Copyright © Nik Zaugg Alex Scheitlin Moritz Eck 2020.

Evaluations Provotum 2.0

- ❑ E2E-Verifiability and Ballot Secrecy achieved ✓
- ❑ Client-Side Cryptography ✓
- ❑ On-Chain Proof Verification ✓
- ❑ Distributed Key Generation ✓
- ❑ Cooperative Decryption ✓

- ❑ Solidity EVM restricted to 256-bit integers ✗
- ❑ Mitigate Identity provisioning scheme threats ✗

- ❑ Receipt-Freeness and Coercion-Resistance ✗

Summary

❑ Remote Electronic Voting

- If trust is distributed in REV, then REV 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 consensus