

Blockchain-based Remote Electronic Voting

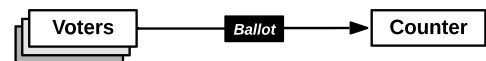


ToC

- 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

Aren't 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

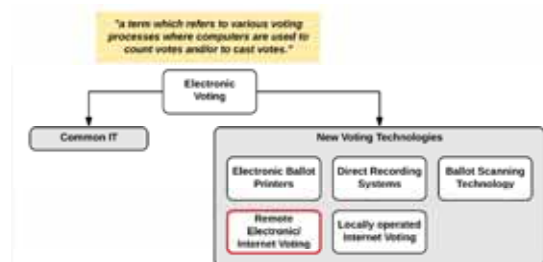
The Secret Ballot

- 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

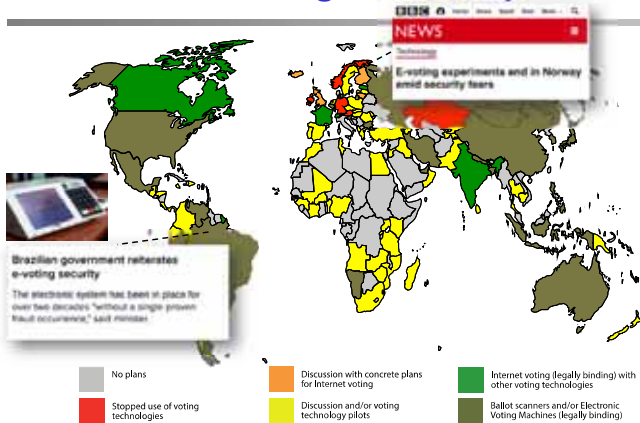


Terminology

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



E-Voting World Map



© 2020 UZH, CSG@ifi

7

Source: e-voting.cc



Estonia



© 2020 UZH, CSG@ifi

8

Source: Security Analysis of the Estonian Internet Voting System, Drew Springall et al., November 2014



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 Trümper Photography, <https://www.gl.ch/landsgemeinde.html/216>

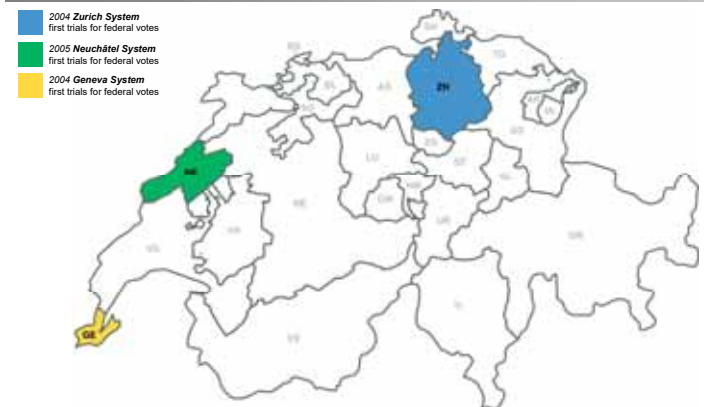
© 2020 UZH, CSG@ifi

9

Source: <https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/chronik.html>



First Trials, Initial Pilot Phase



© 2020 UZH, CSG@ifi

10



Extension of Trials

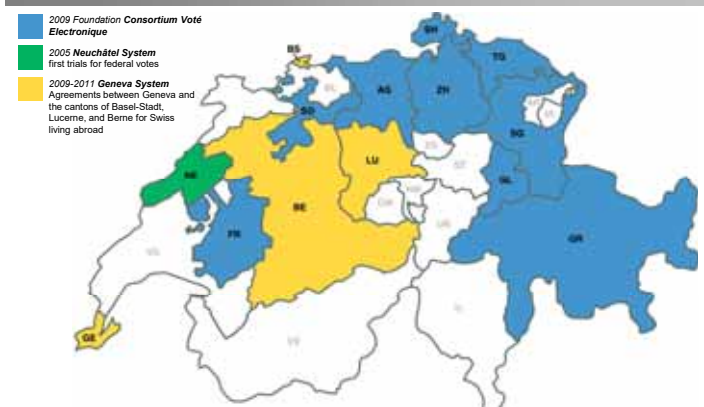
- In 2006, the Federal Government opened the door for all cantons to use *limited* internet voting:
 - 20% of the cantonal electorate (later extended to 30%);
 - 10% of the federal electorate
- Geneva and Zurich (Vote Consortium) started offering their system to other cantons
 - Some drawbacks were also experienced:
 - Regulatory issues in Geneva (2005 – 2007)
 - Technical issues in Zurich (2011 – now)

© 2020 UZH, CSG@ifi

11



Extension of Swiss-wide Pilots



© 2020 UZH, CSG@ifi

12



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

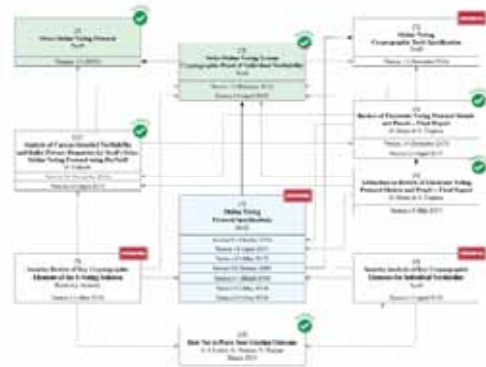
Level	Limit ¹⁾	Requirements	Certification
1	50% maximal 10% Swiss	Technical and security – ISO Common Criteria EAL by – Internet Voting Products – Federal of Europe standards	– Swiss and ECV experts assessment of – documentation (risk assessment, security architecture, ...) and security tests of system – hardware and infrastructure
2	50% maximal 50% Swiss	Individual verifiability – Certificate-based verifiability – Receipt-based verifiability	– Security (Common Criteria EAL 3) – Cryptography: Security and formal proofs – printing, server and tally are trusted – infrastructure and printing offices
3	Not set	Complete verifiability – Individual verifiability – Receipt-based verifiability – Certificate-based verifiability – Certificate-based verifiability	– Security (Common Criteria EAL 4) (EAL 4 control component) – Cryptography: Security with formal proofs – printing and end-point components and business – 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



sVote Dependencies



Advertisement on Public Initiative



Swiss public initiative on a “Secure and trusted democracy”



Proposed Law

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

Art. 101 Abs. 1

1. Übergangsbestimmung zu Art. 99 Abs. 1¹⁾ (Verwendung elektronischer Verfahren zur Stimmabgabe)

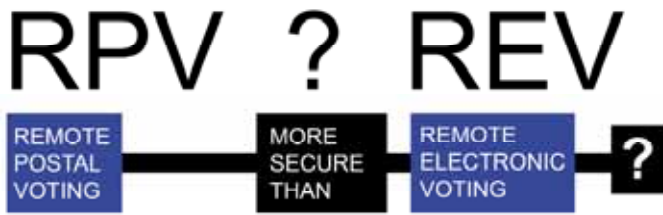
¹⁾ Artikel 99 Absatz 1 tritt mit der Annahme durch Volk und Stände in Kraft, mit der Annahme sind sämtliche Bestimmungen des kantonalen Rechts und des Bundesrechts über elektronische Verfahren zur Stimmabgabe nicht mehr anwendbar.

²⁾ Die Bundesversammlung kann den Vorbehalt durch Bundesgesetz verheissen, wenn

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“

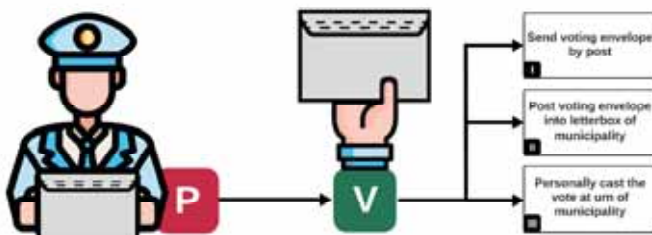


The Swiss RPV Case

- 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

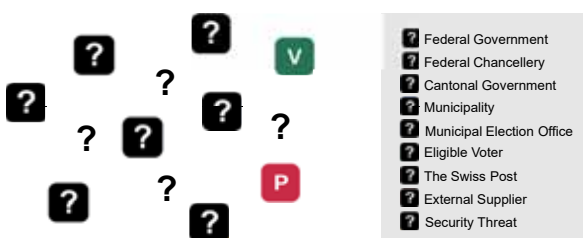


RPV: Remote Postal Voting

PVPF: Postal Voting Process Flow

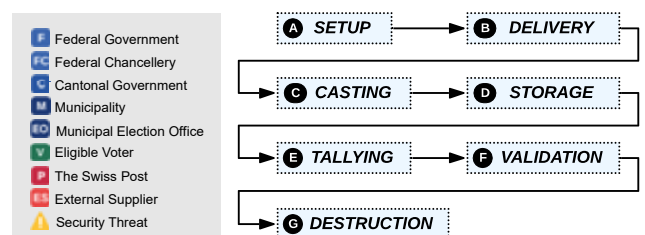


Identification of Stakeholders



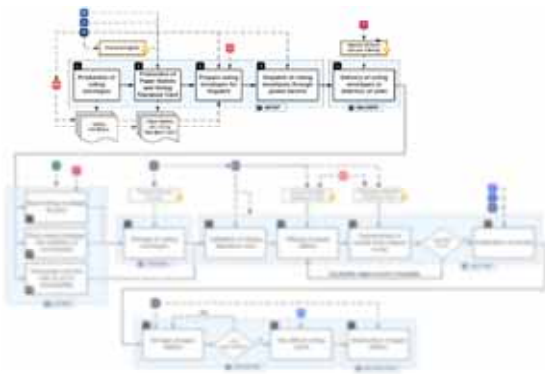
PVPF Phases

- Divided into phases A to G with various stakeholders



PVPF: Postal Voting Process Flow

PVPF in Detail



[KS19]

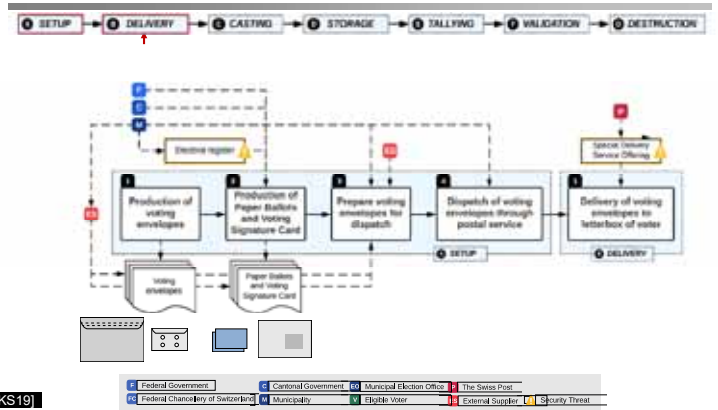
PVPF: Postal Voting Process Flow

© 2020 UZH, CSG@IFI

25



A: Setup, B: Delivery



[KS19]

© 2020 UZH, CSG@IFI

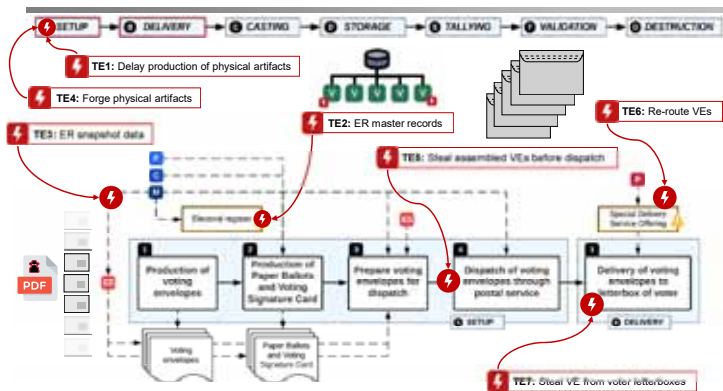
26



A: Setup, B: Delivery



THREAT EVENTS

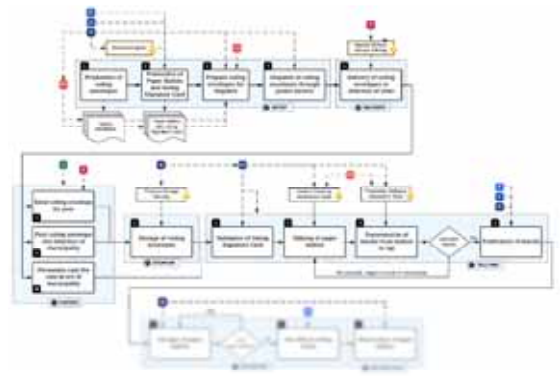


© 2020 UZH, CSG@IFI

27



PVPF in Detail



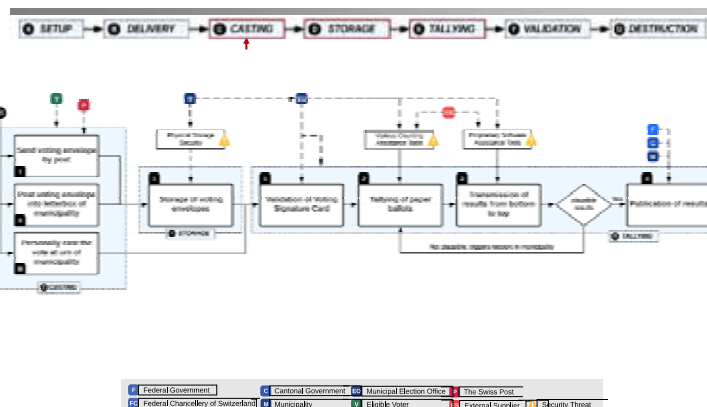
PVPF: Postal Voting Process Flow

© 2020 UZH, CSG@IFI

28



C: Casting, D: Storage, E: Tallying



© 2020 UZH, CSG@IFI

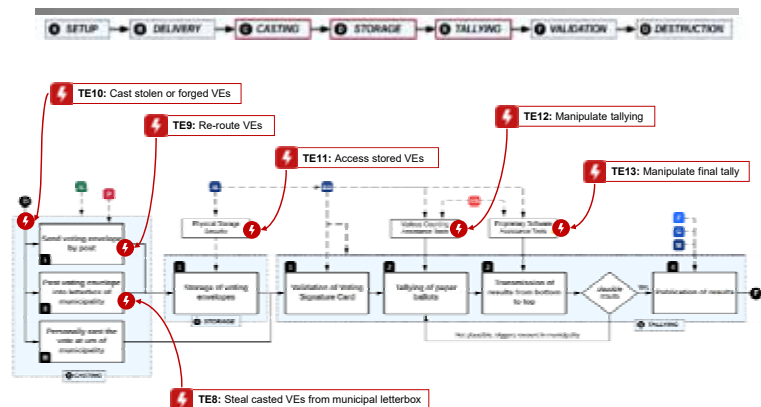
29



C: Casting, D: Storage, E: Tallying



THREAT EVENTS

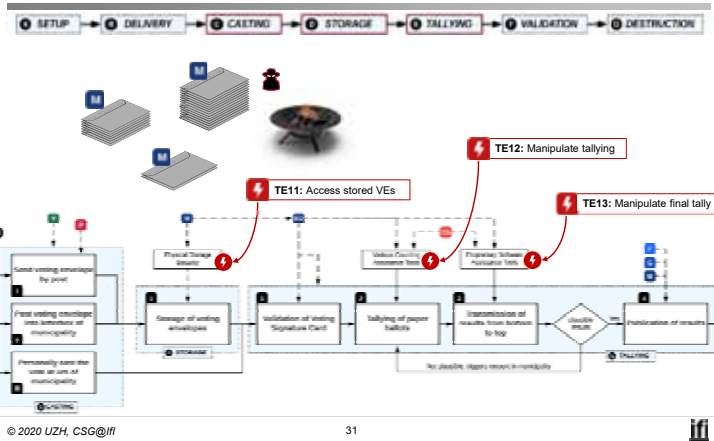


© 2020 UZH, CSG@IFI

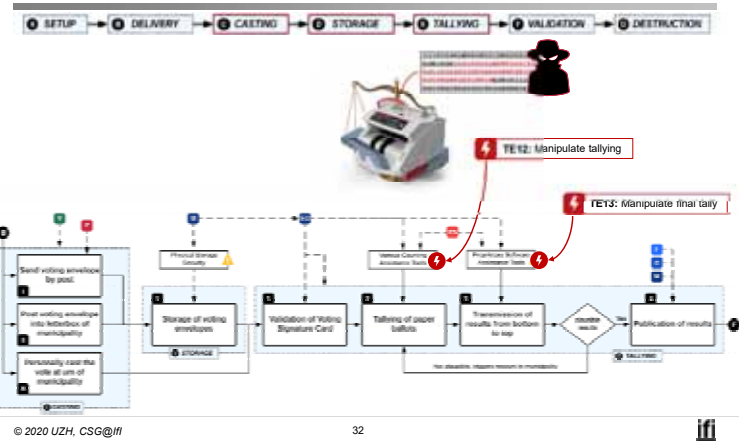
30



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

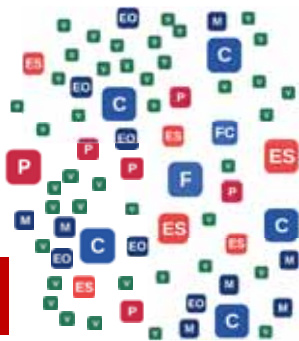


C: Casting, D: Storage, E: Tallying THREAT EVENTS



Conclusions on the Swiss RPV

Heterogeneous Processes



Distribution of Trust and Physical Decentralization

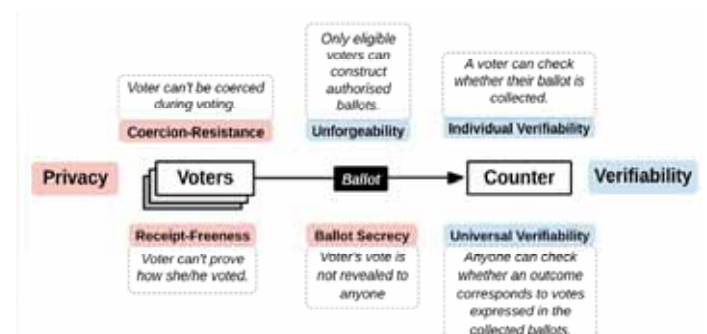
Substantial Trust in Third Parties

Theoretical Properties

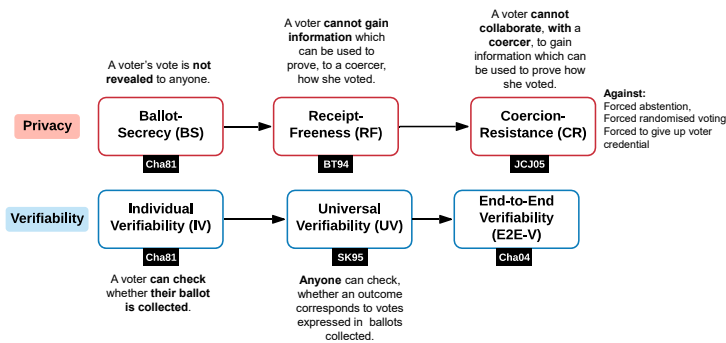
REV Requirements

- 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



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
 - Talled 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

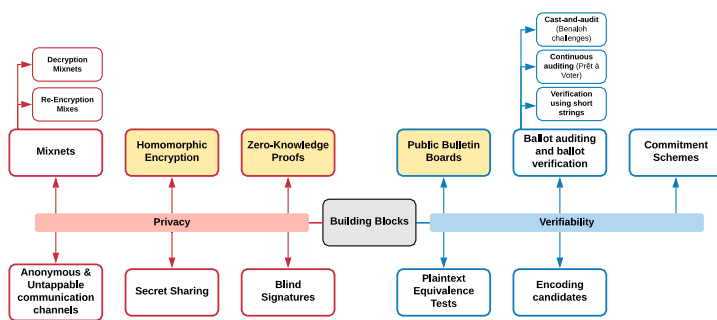
Refinements of Software Independence

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

Based on 'Privacy and Verifiability in Voting Systems' by H. Jonker 2013

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!

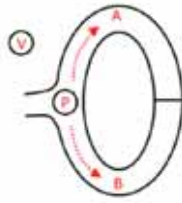
- Each voter proves that she cast a valid vote, without revealing her/his vote
- The authorities prove that they know their secret keys (that match the election public keys), without revealing their secret keys
- At the end of the election, the authorities prove that they have tallied correctly (decrypted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

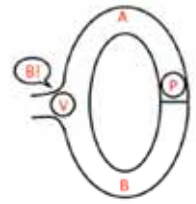
Ali Baba's Cave (1)

- 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



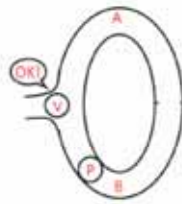
Ali Baba's Cave (2)

- 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

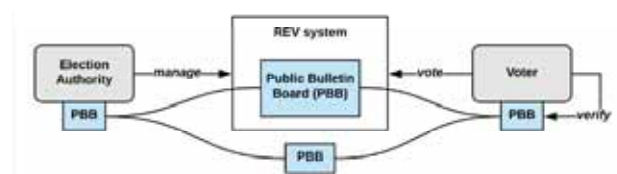
➤ *How can voters verify the election data?*

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

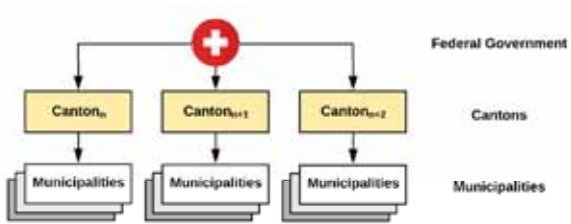
Public Permissioned Blockchain (BC)

- **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



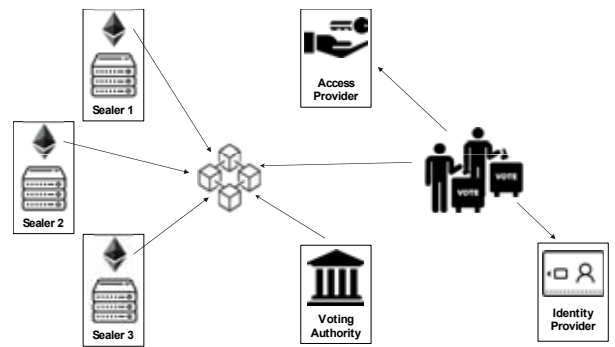
KRM201

© 2020 UZH, CSG@ifi

55



BC-based REV System: *Provotum*

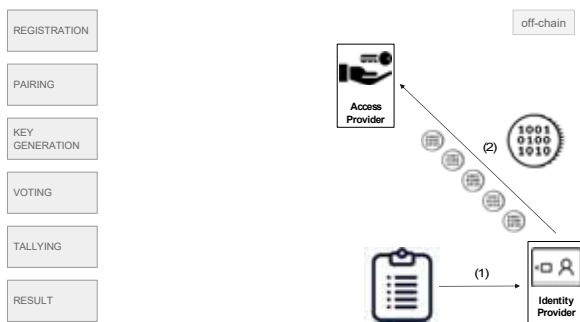


© 2020 UZH, CSG@ifi

56



Provotum 2.0 Identity Provisioning

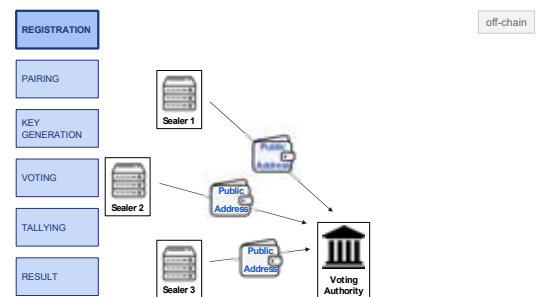


© 2020 UZH, CSG@ifi

57



Voting Protocol: Registration (1)



© 2020 UZH, CSG@ifi

58



Voting Protocol: Registration (1)

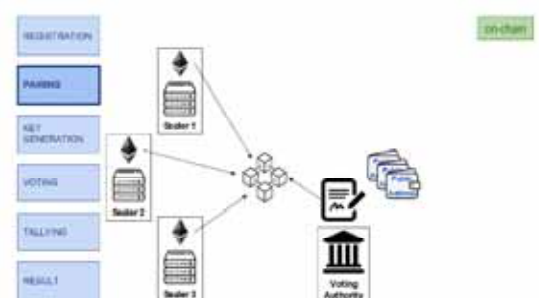


© 2020 UZH, CSG@ifi

59



Voting Protocol: Pairing (2)



© 2020 UZH, CSG@ifi

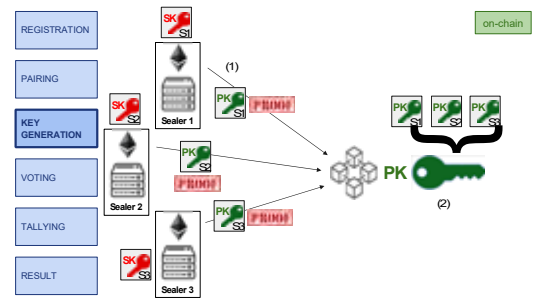
60



Voting Protocol: Pairing (2)



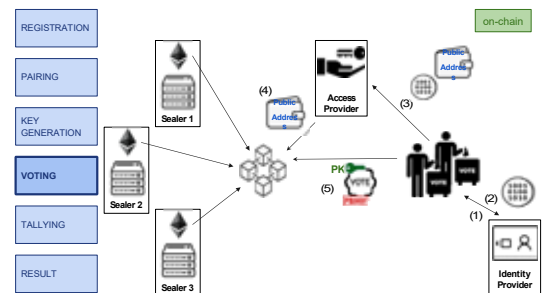
Voting Protocol: Key Generation (3)



Voting Protocol: Key Generation (3)



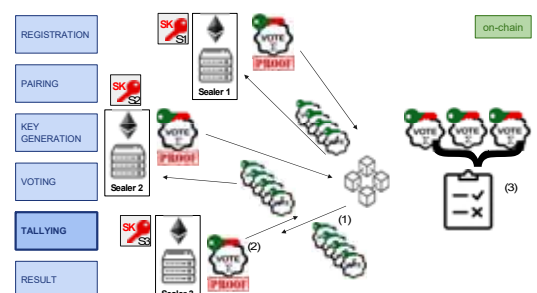
Voting Protocol: Voting (4)



Voting Protocol: Voting (4)



Voting Protocol: Tallying (5)



Voting Protocol: Tallying (5)



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