BAT 2017

E-Voting - Herausforderung an Kryptographie und Praxis

Stephan Fischli, Philipp Locher, Benjamin Fankhauser

e-voting.bfh.ch

3. November 2017

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Einführung

Tages-Anzeiger

Front Zürich Schweiz International Wirtschaft Börse Sport Kultur Reisen Wissen Auto Blogs Panorama Mehr

SonntagsZeitung // ePaper Leserangebote Leserreisen Leserbriefe Monatsquiz Abonnieren

E-Voting: Unsicheres System und Maulkorb für Kritiker

Befürworter elektronischer Abstimmungen wie FDP-Nationalrat Marcel Dobler wollen die Technologie auf Teufel komm raus durchboxen.

netzwoche

NEWS STORYS MEINUNGEN STUDIEN DOS

NEWS

Zertifizierung erweitert

Post kann E-Voting für 50 Prozent der Stimmbürger anbieten

Mo 21.08.2017 - 10:23 Uhr | Aktualisiert 21.08.2017 - 10:23
von Christoph Grau

Bisher durften mit der E-Voting-Lösung der Post nur 30 Prozent der Stimmbürger elektronisch abstimmen. Die Bundeskanzlei hob die Grenze nun auf 50 Prozent an. In einem Jahr sollen es 100 Prozent werden.

HOME ABO E-PAPER/HEFTARCHIV EVENTS NEWSLETTER RSS-FEED MEDIADATEN KONTAKT

Computerworld

Google Benutzerdefinierte Su

Webcode Computerworld.ch Web

NEWS BUSINESSPRAXIS TESTS MARKTANALYSEN JOB & KARRIERE WHITEPAPERS SERVICE PARTNERZONEN

Home » News » Security

Twittern +1 Gefällt mir XING Share

E-Voting: Wie sicher sind die Schweizer Lösungen?

Wie sicher sind die Schweizer E-Voting-Systeme? Diese Frage beschäftigt nicht nur die Politik, sondern auch die IT-Security-Szene. So widmete sich auch ein Themenblock am diesjährigen SwissCyberStorm in Luzern der elektronischen Stimmabgabe.

Einführung

- Warum sprechen wir (immer noch) über E-Voting?
  - → Hohe Anforderungen:
    Korrektheit + Verifizierbarkeit + Wahlgeheimnis
  - → Komplexe Systeme (fachlich/technisch/organisatorisch)
- Brauchen wir überhaupt E-Voting?
  - → Digitale Gesellschaft
  - → Enabling Technologie (z.B. Auslandschweizer)
  - → Kostenersparnis

Umfeld

- Privater Bereich
  - → Firmen, Pensionskassen, Vereine
  - → Unterschiedliche Sicherheitsanforderungen
- Öffentlicher Bereich
  - → Bund, Kantone, Gemeinden
  - → Höchste Sicherheitsanforderungen (z.B. sichere Endgeräte)
  - → Aktuell 8 Kantone mit Grundbewilligung und 2 produktive Systeme (Genf und Post)
  - → Überführung der Versuchsphase in Normalbetrieb

E-Voting Gruppe der BFH

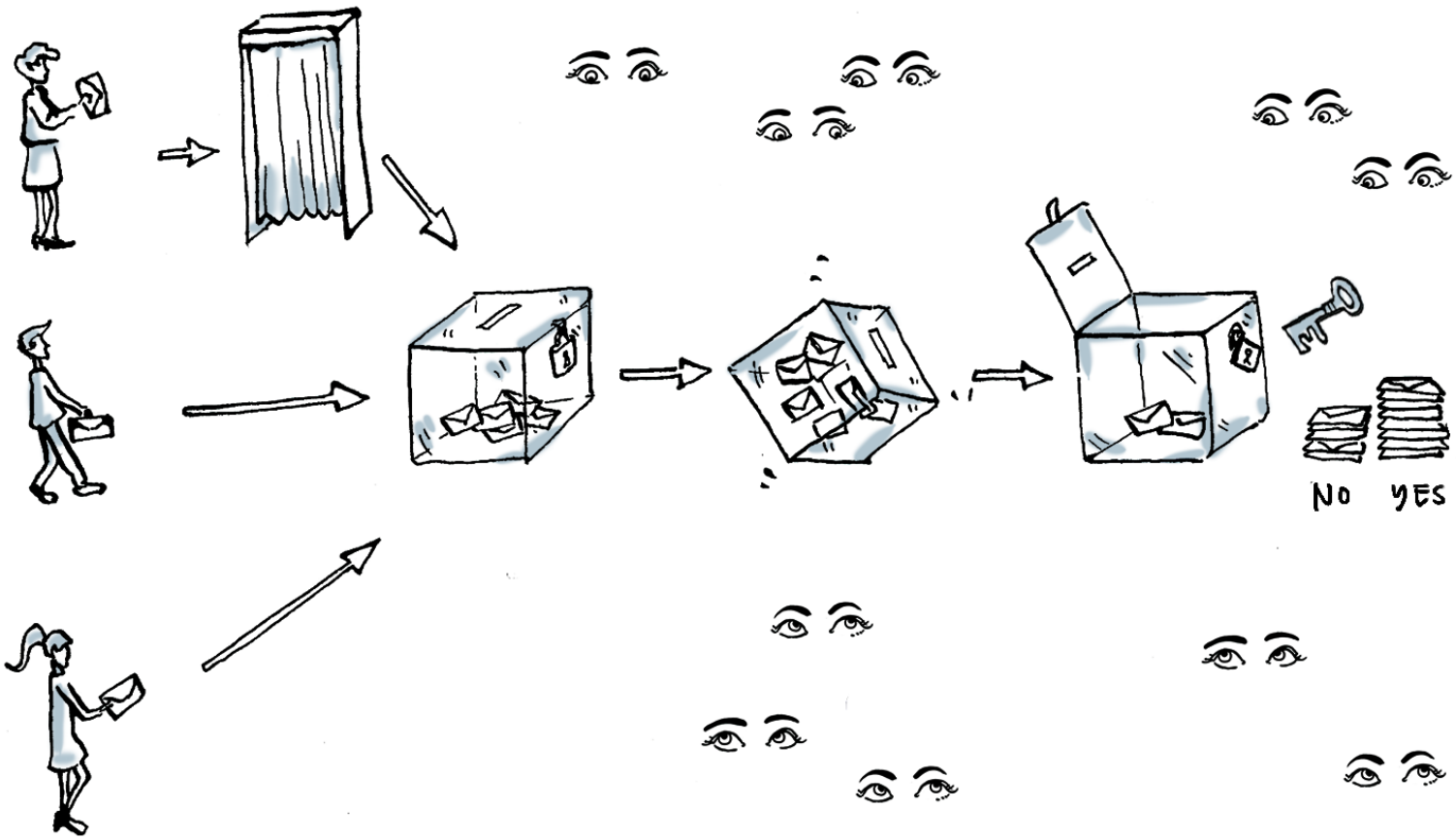
- Forschung zu E-Voting (kryptographische Protokolle)
- Zusammenarbeit mit
  - → Bundeskanzlei
  - → Kantonen
  - → Systemanbieter
  - → Firmen
- PoC mit UniVote für Studentenratswahlen Schweizer Universitäten
- Vollständig verifizierbares E-Voting Systems für den nicht-öffentlichen Bereich

Einführung

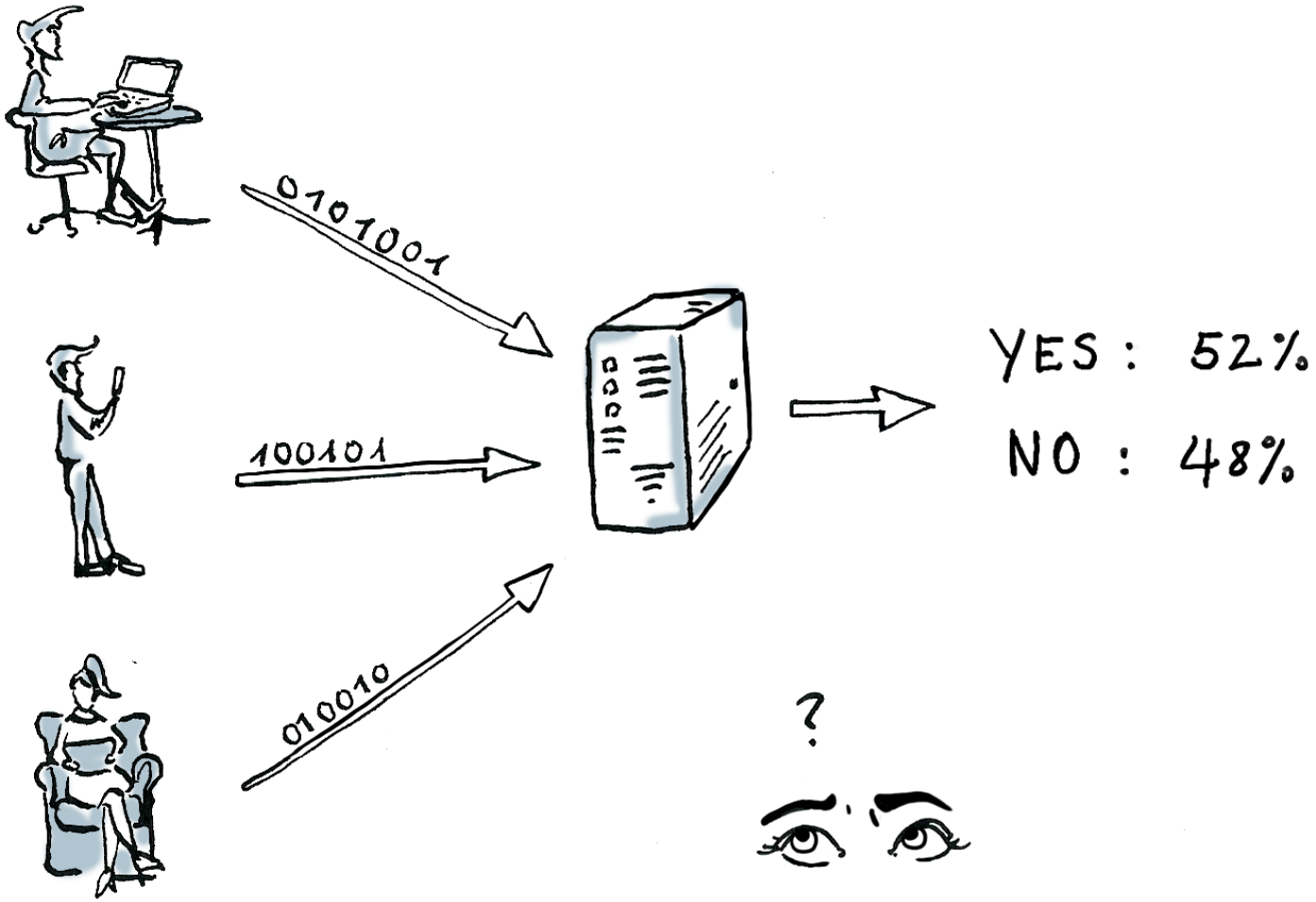
Kryptographie

Praktische Aspekte

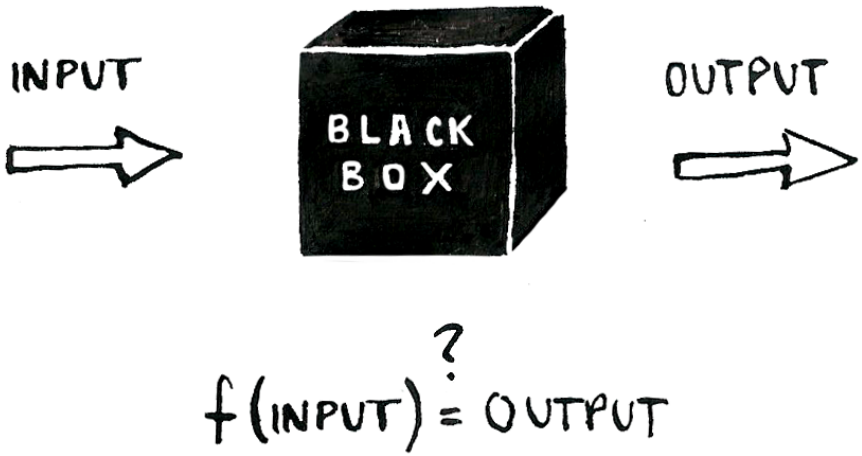
Traditionelles papierbasiertes Abstimmen



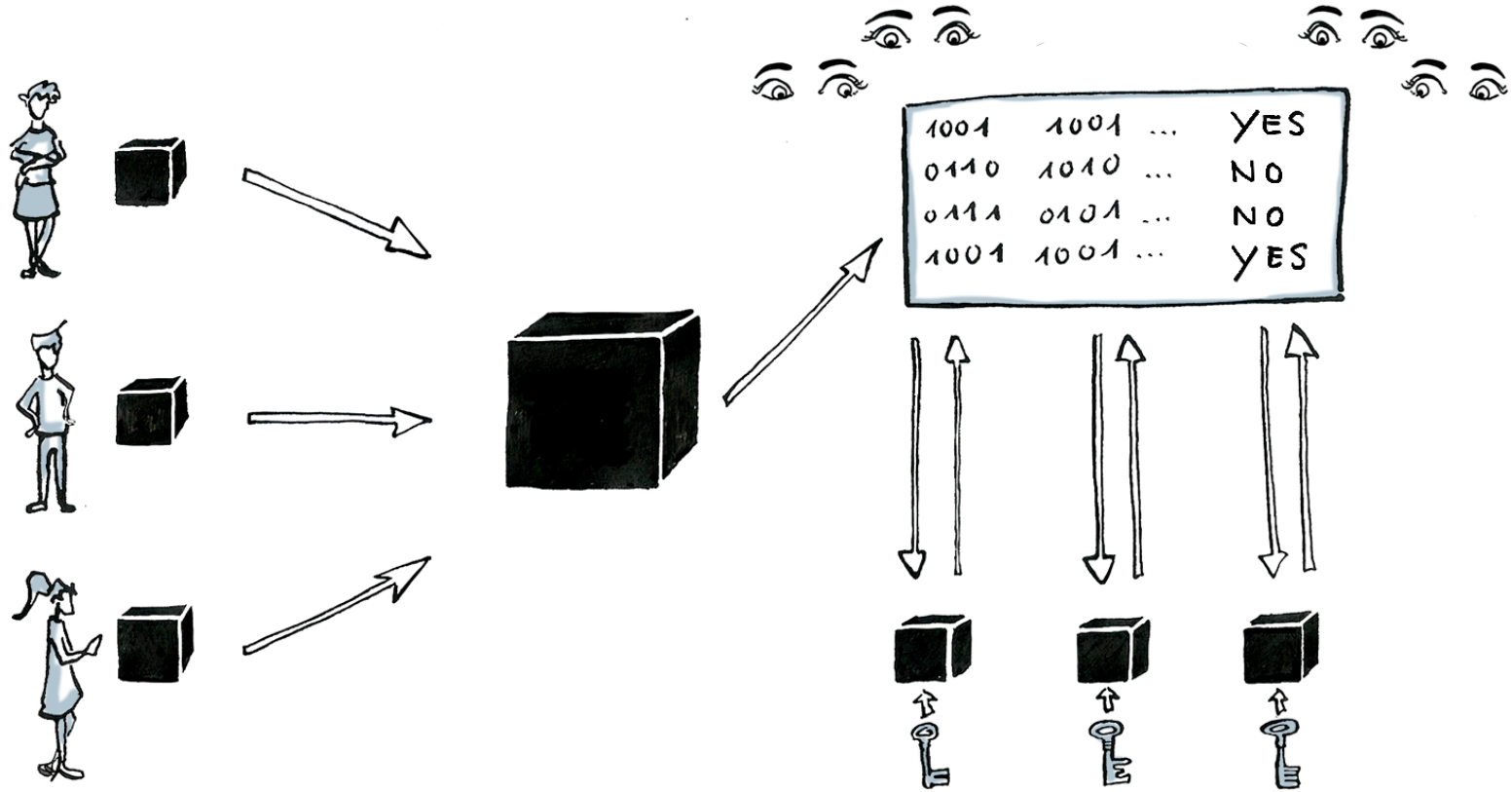
Remote E-Voting



End-to-End Verifizierbarkeit



Verifizierbares E-Voting



Eigenschaften eines E-Voting Systems

Verifizierbarkeit Das finale Resultat kann verifiziert werden (Kombination aus individueller und universeller Verifizierbarkeit)

Wahlgeheimnis Das Wahlgeheimnis ist garantiert, wenn möglich für immer und bedingungsslos

Angriffsresistenz Ein Erpresser oder Betrüger kann den Wähler nicht für ihn überprüfbar beeinflussen

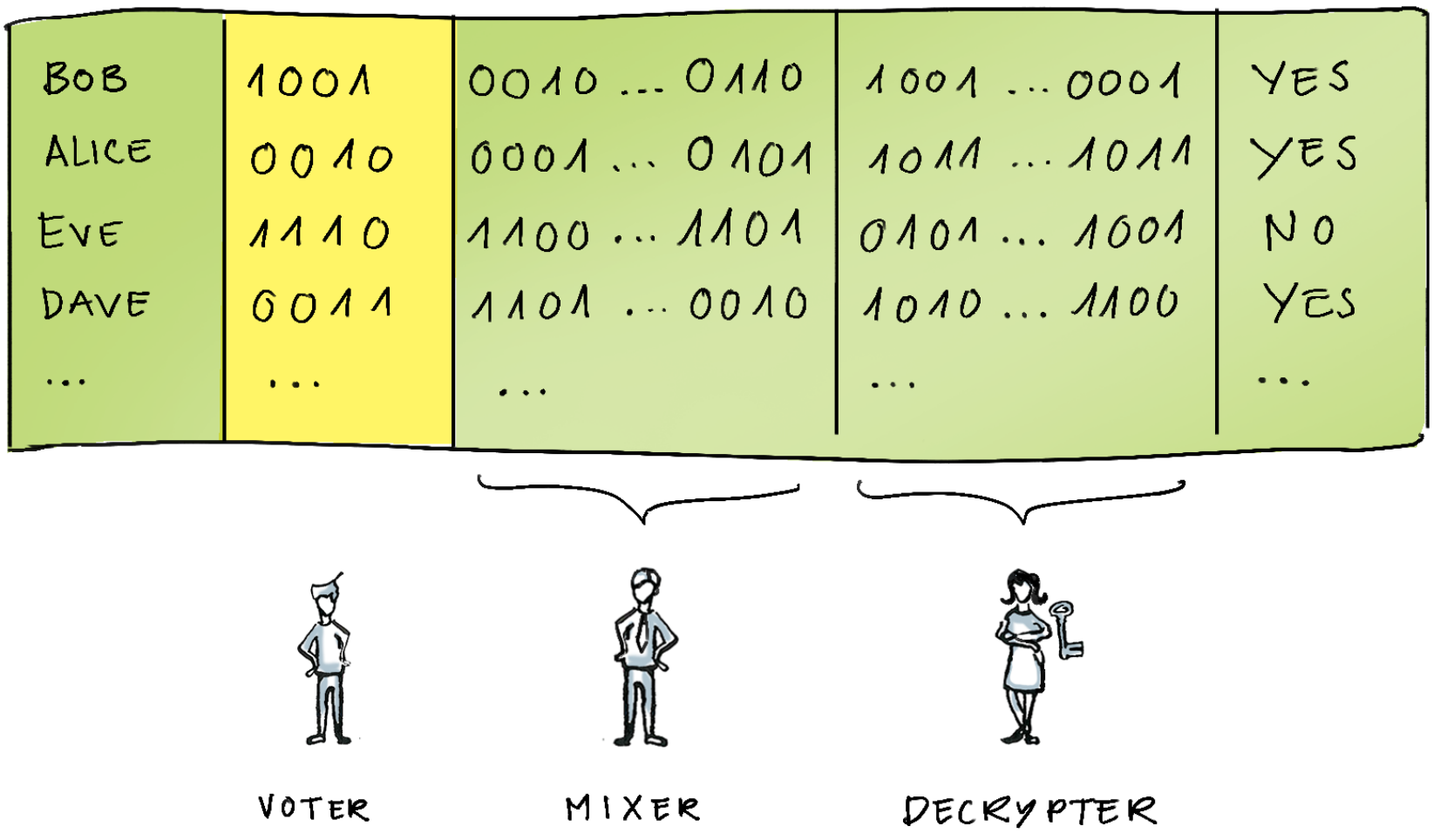
Bulletin Board

Abstimmung Nationalrat (srf.ch)

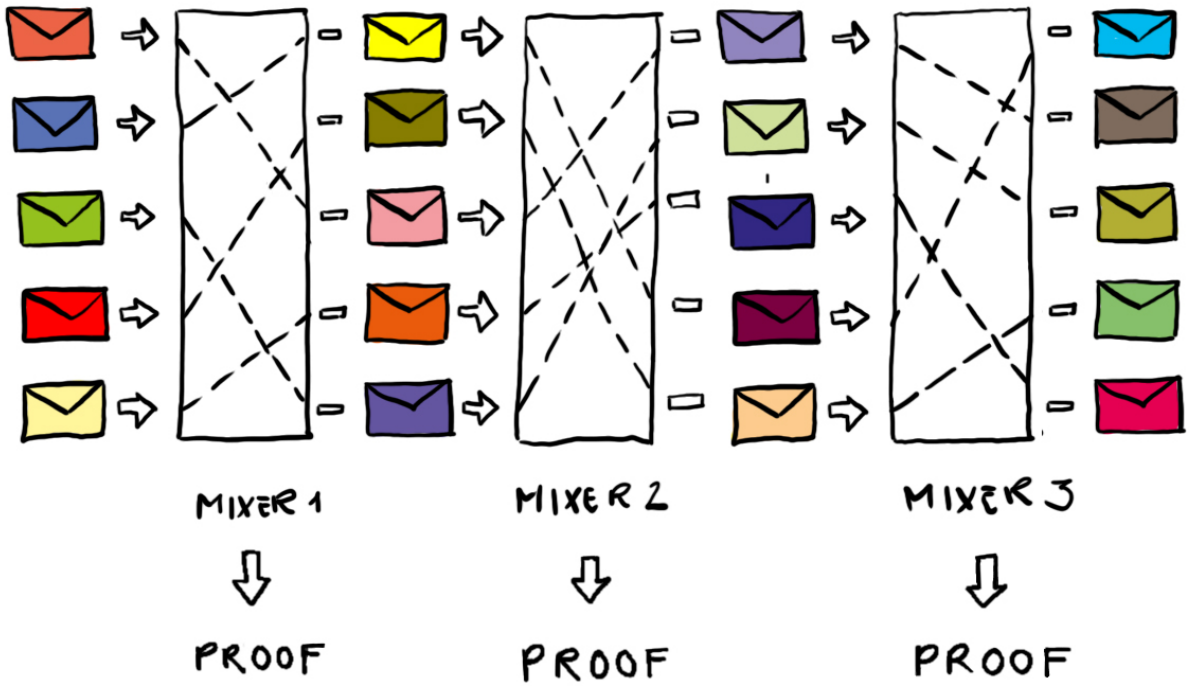
Bulletin Board

Namensliste der Stimmberechtigten, Erbil 2017 (nzz.ch)

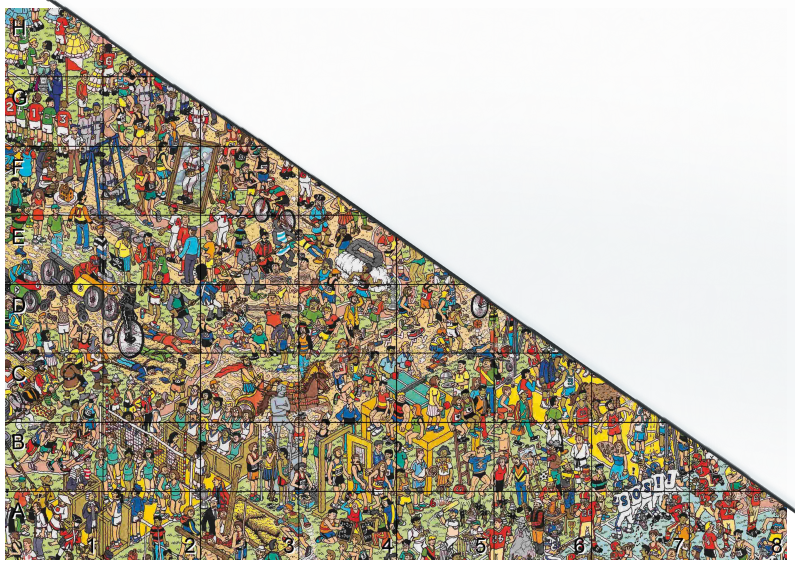
Bulletin Board



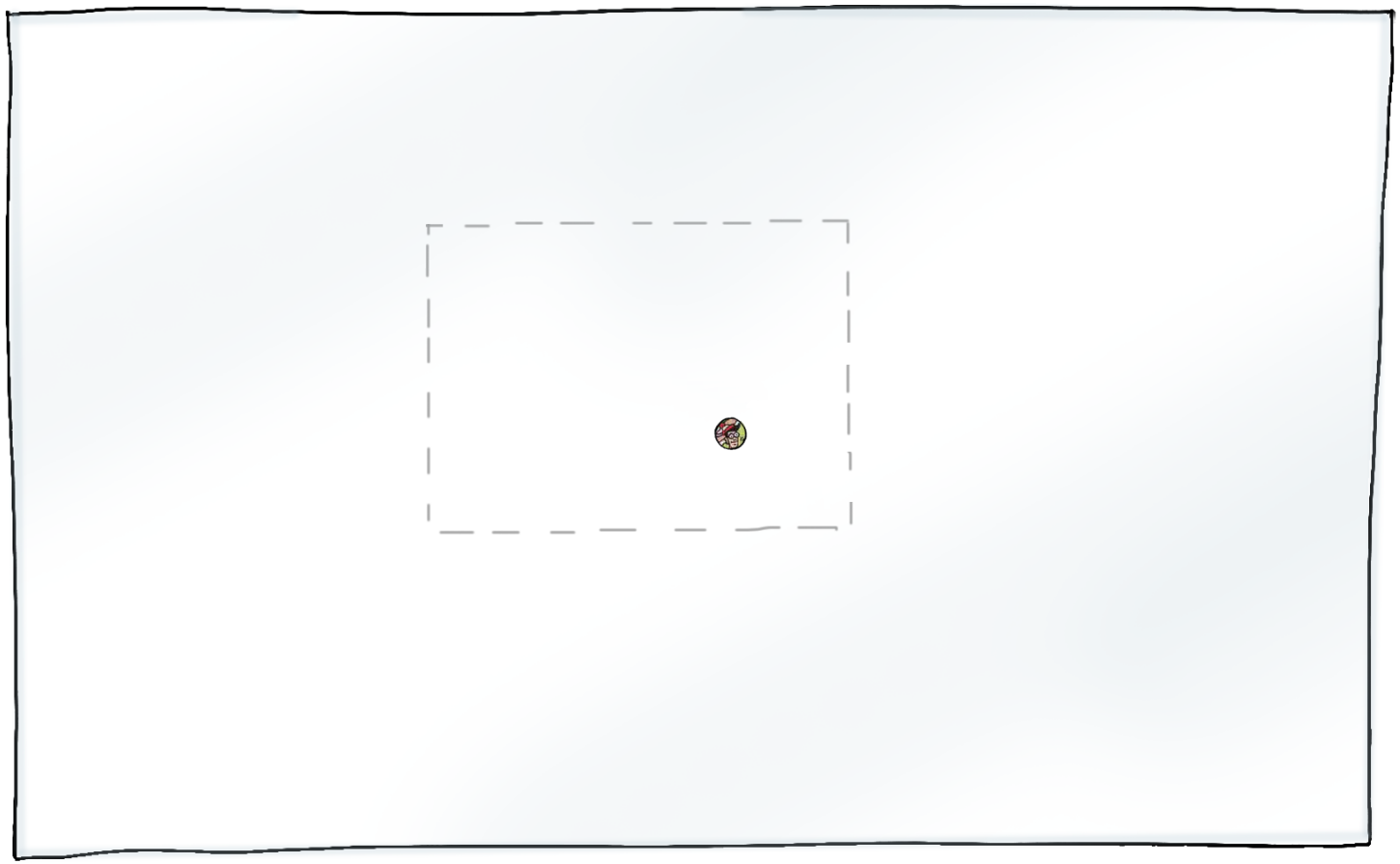
Mix-Net



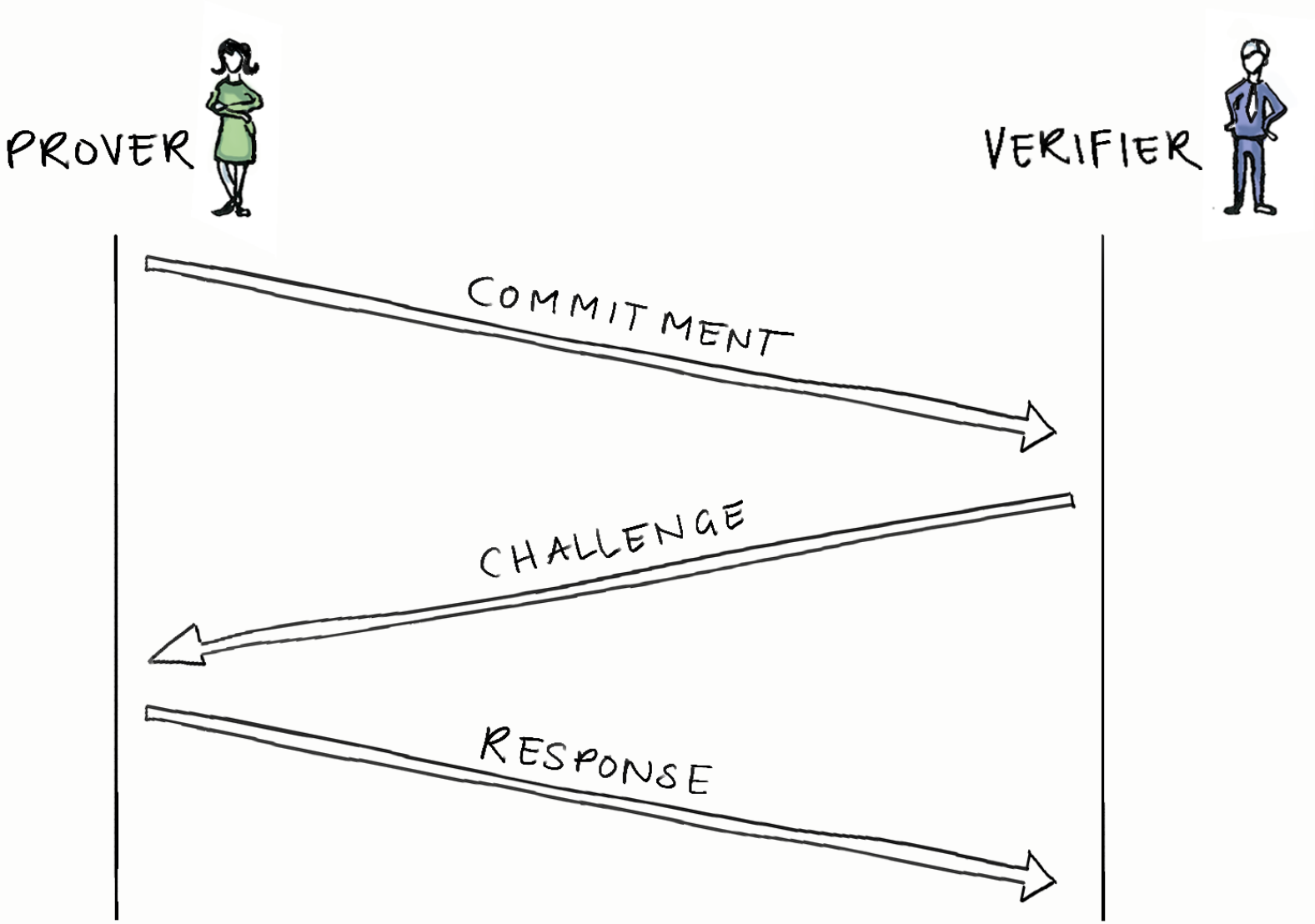
Zero-Knowledge Proof



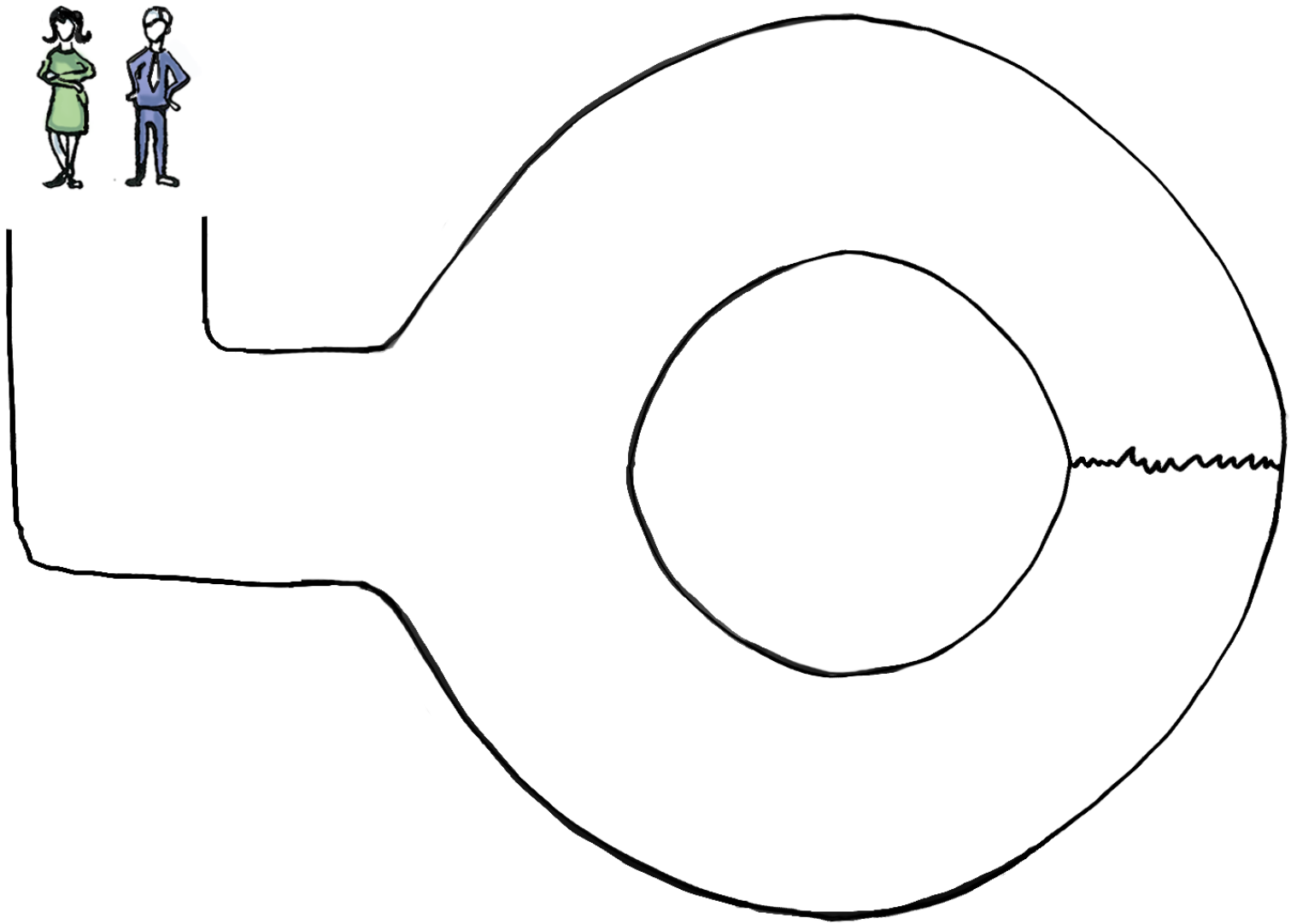
Zero-Knowledge Proof



Zero-Knowledge Proof



Zero-Knowledge Proof

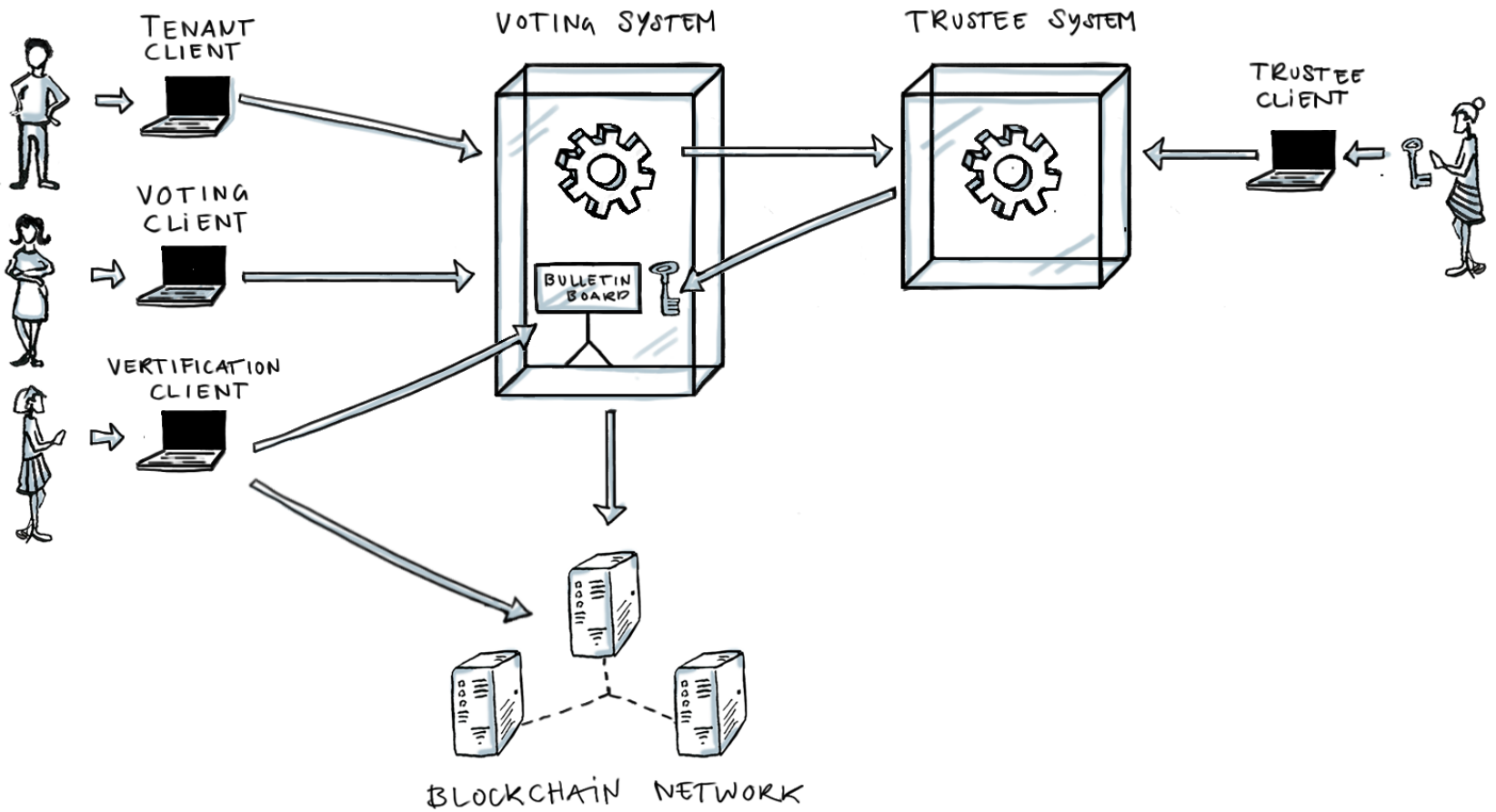


Einführung

Kryptographie

Praktische Aspekte

Architektur



Demo