Voting and Blockchain: Promise and Challenges

Prof. Bryan Ford
Decentralized and Distributed Systems (DEDIS)
School of Information and Communications (IC)
dedis@epfl.ch – dedis.epfl.ch

Geneva Blockchain Congress – January 20, 2020

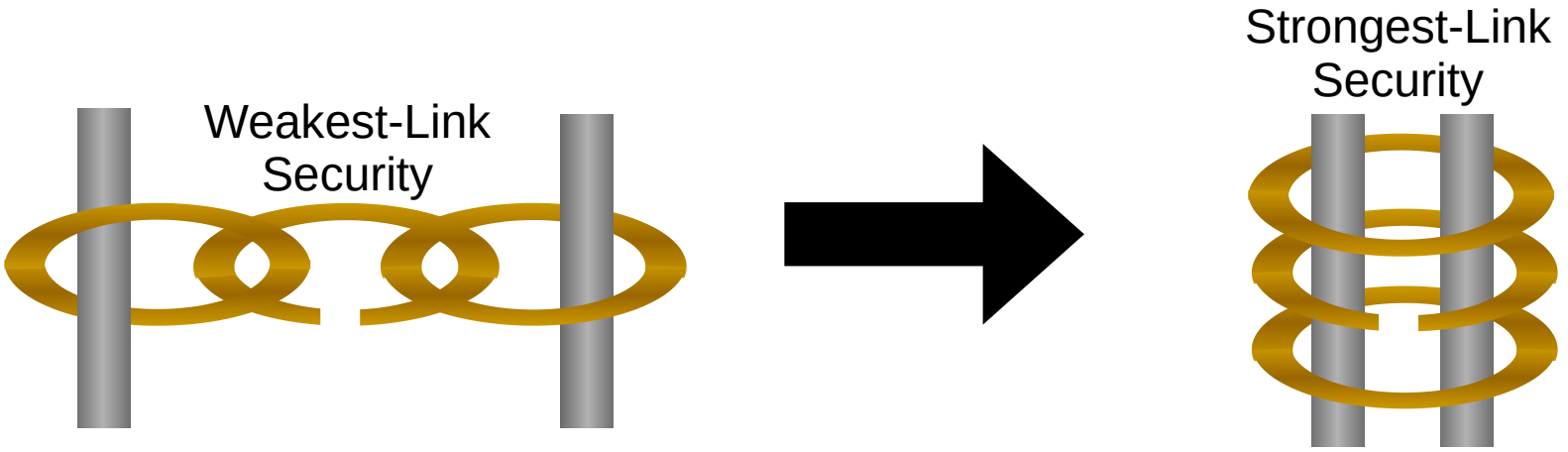
The DEDIS lab at EPFL: Mission

Build advanced **Decentralized and Distributed Systems (DEDIS)**

- **Distributed:** spread widely across the Internet & world
- **Decentralized:** independent participants, no central authority, no single points of failure or compromise

Systems that **distribute trust** widely with **strongest-link security**

Website: **https://dedis.epfl.ch**



Talk Outline

- The appeal and history of E-voting
- What's missing: key unsolved challenges
  - Keeping secrets off- or on-chain
  - Transparency versus long-term privacy
  - Coercion and vote-buying
- Conclusion: there's promise, but be cautious

Talk Outline

- **The appeal and history of E-voting**
- What's missing: key unsolved challenges
  - Keeping secrets off- or on-chain
  - Transparency versus long-term privacy
  - Coercion and vote-buying
- Conclusion: there's promise, but be cautious

E-voting: the Convenience Appeal

Convenience of vote from home (or anywhere)

- Ideally with whatever device you prefer

E-voting: the Participation Appeal

Allow **rich, frequent** participation by constituents

- While maintaining or **improving** voter turnout

E-voting: the Scalability Appeal

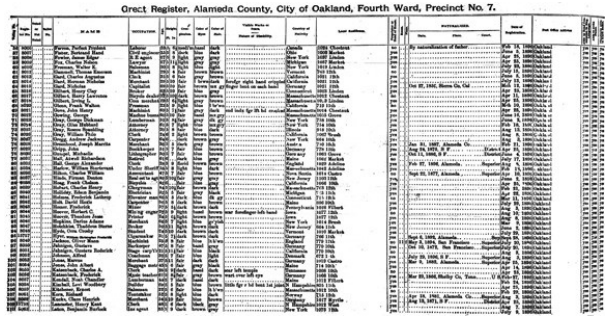
Mass online deliberation, liquid democracy

E-voting: a Generic Workflow

Three fundamental phases:

- Registration, credential creation and renewal
- Vote casting and recording
- Results tallying and publication

Sounds like a process that could use a **ledger**?



E-voting and Blockchain

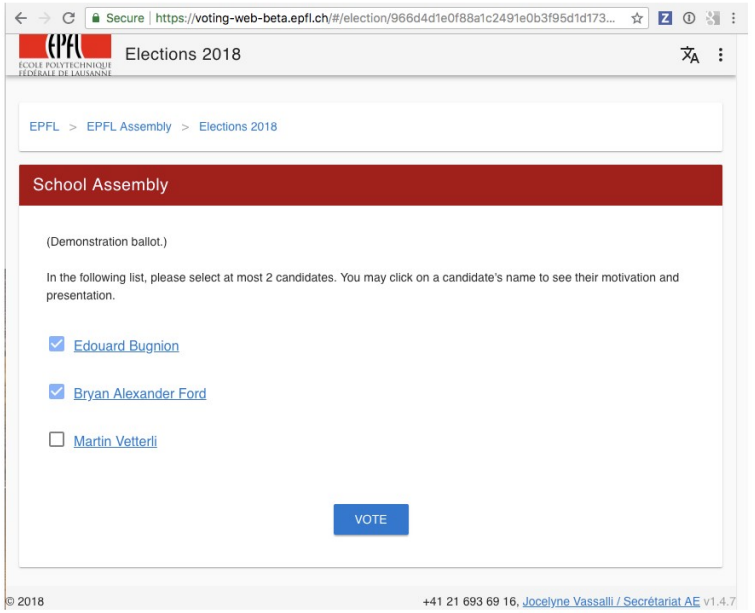
You can record **anything** on a blockchain, right?

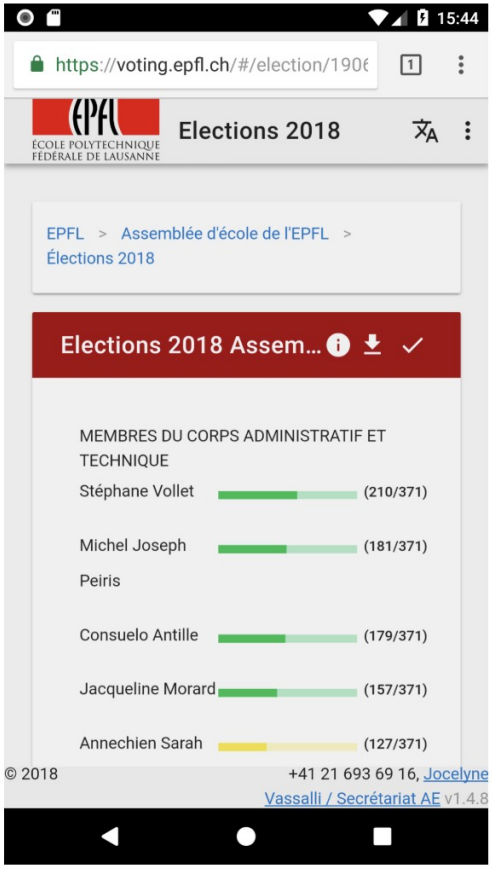
- So why not cast & count votes on a blockchain?

Blockchain E-voting: Yes We Can

We do for EPFL Assembly elections since 2018

- DEDIS system serving ~10,000 eligible voters
  - https://blog.dedis.ch/post/evoting/
- Builds on DEDIS's **Calypso** blockchain design

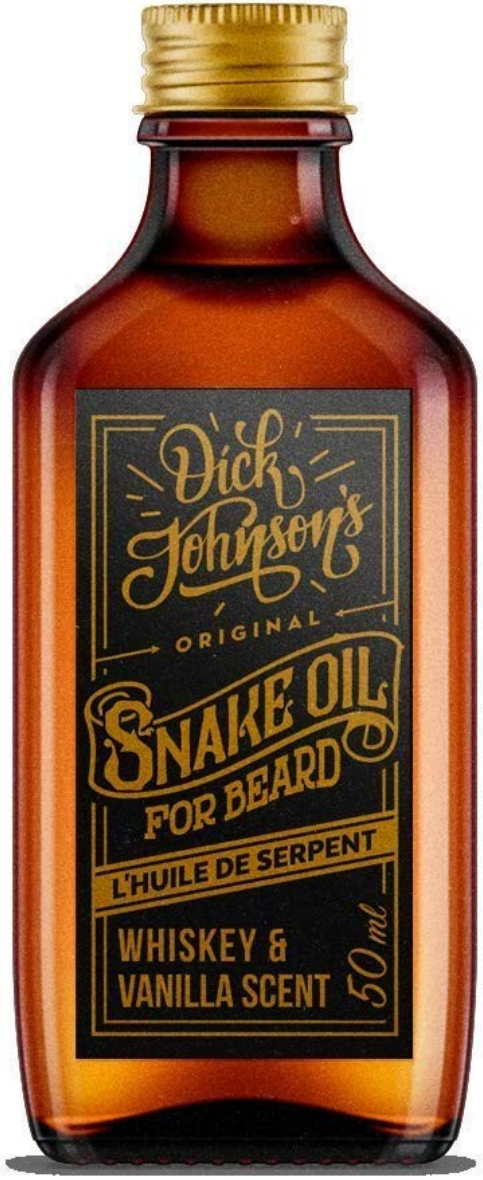




But *hold on*…

Not to rain on the parade, but…

Blockchain won’t magically make E-voting safe or secure



E-voting tech has used “blockchain” since long before “blockchain”

Decades-old cryptographic tools, such as:

- Merkle trees and hash authentication: **1988**
- Distributed ledgers and time-stamping: **1990**
- Verifiable shuffles for voting privacy: **2001**
- First public E-voting in Switzerland: **2003**
- Practical voter-verifiable elections: **2004**

(Bitcoin: **2008**; “Blockchain”: **later**)

Example: Swiss vs EPFL E-voting

Blockchain-based EPFL system suited for internal low-stakes use, *not* for large-scale public elections

		EPFL
Protection from compromised voting device (“cast-as-intended”)	✓	
End-to-end voter verifiability (“recorded-as-cast”)	✓	✓
Auditable vote counting (“counted-as-recorded”)	✓	✓
Decentralized verification with no single points of failure (“cothority”)		✓

Talk Outline

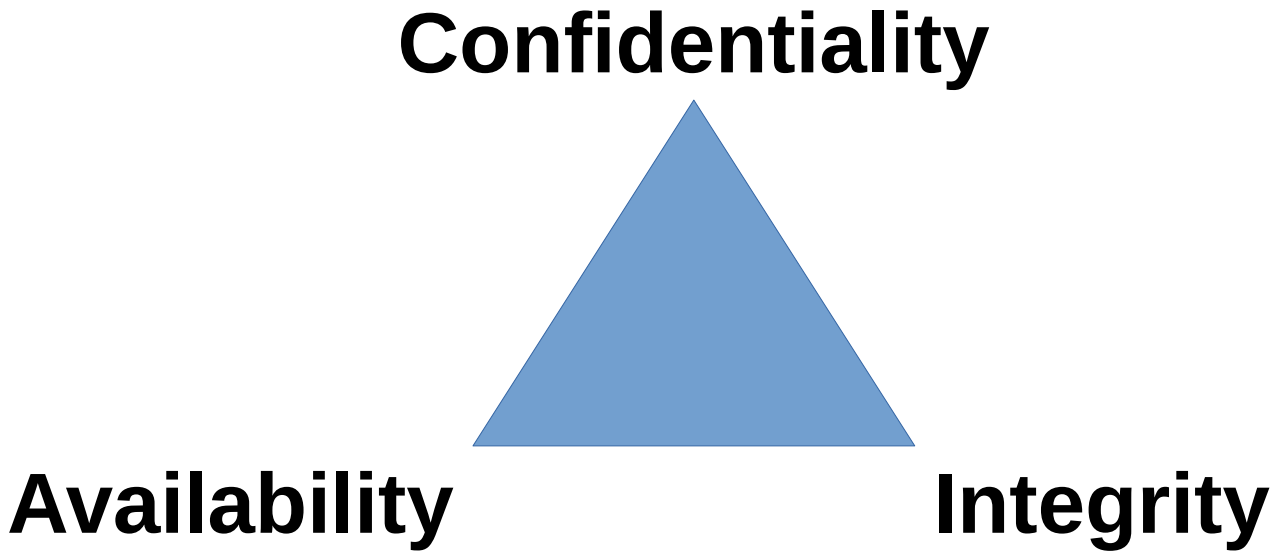
- **The appeal and history of E-voting**
- What's missing: key unsolved challenges
  - Keeping secrets off- or on-chain
  - Transparency versus long-term privacy
  - Coercion and vote-buying
- Conclusion: there's promise, but be cautious

Talk Outline

- The appeal and history of E-voting
- **What's missing: key unsolved challenges**
  - **Keeping secrets off- or on-chain**
  - Transparency versus long-term privacy
  - Coercion and vote-buying
- Conclusion: there's promise, but be cautious

The C-I-A (or A-I-C) Principle

In information security and data protection, we generally want **three fundamental properties**



Blockchains **strengthen** Integrity and Availability, while by default **weakening** confidentiality!

The Blockchain Privacy Challenge

Blockchains protect the **integrity** of data by *giving everyone a copy* for independent checking

- This works *against* **confidentiality**

Current practice: keep secrets *off-chain*

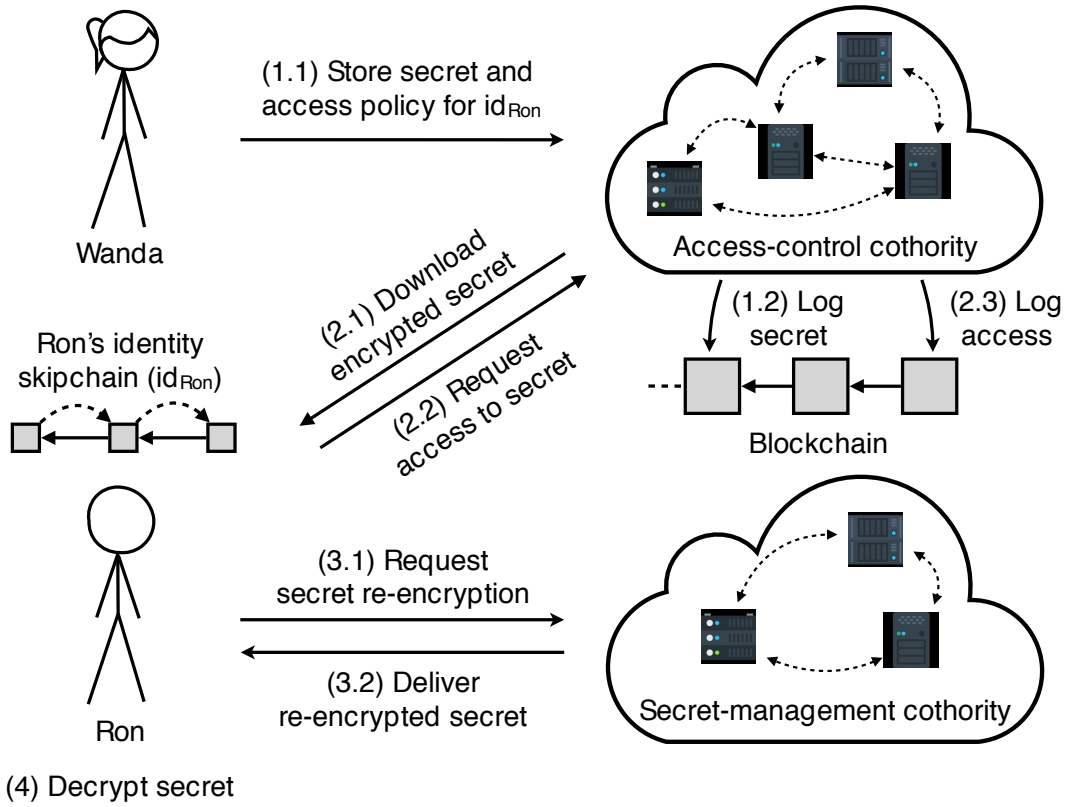
- Only *hashes* or *zero-knowledge proofs* *a*bout those secrets go on-chain
- But user's device – or central trustee – must reveal when required, (e.g., to tally votes)

DEDIS Calypso: on-chain secrets

Verifiable management of private data [arXiv]

Encrypt(*) secrets *care-of the blockchain itself*, under a specific access policy or smart contract

- Threshold of trustees mediate all accesses
- Enforce policies, access recording
- Ensure data both *hidden* and *disclosed* when policy requires
- Can *revoke* access if policy/ACLs change



(*) with post-quantum security if desired

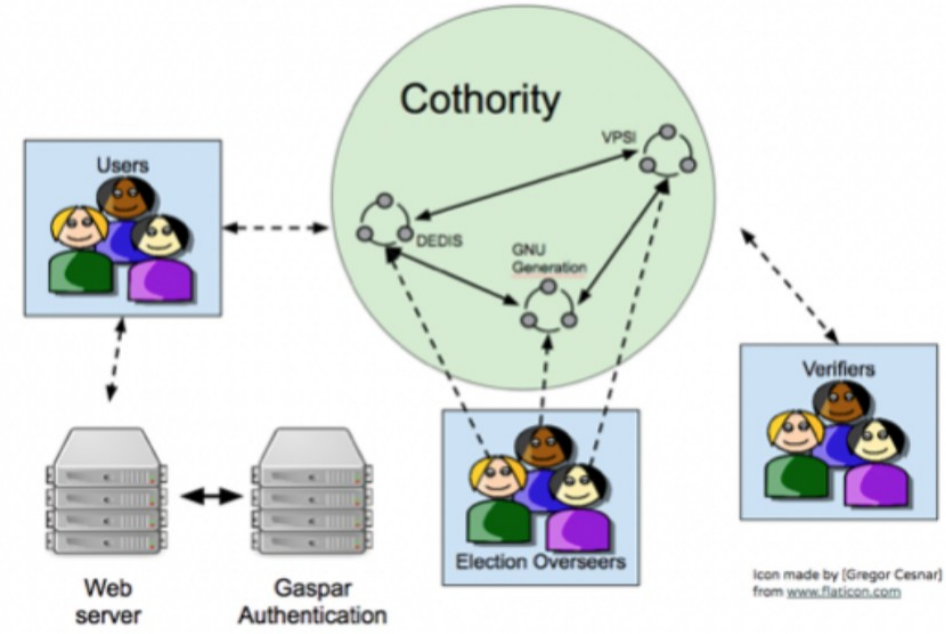
Application to Blockchain E-voting

Basis of EPFL's blockchain-based e-voting system

- State-of-the-art cryptographic security/privacy
- Deployed within EPFL community of 10,000+

Helios-like workflow:

- Clients encrypt votes to threshold of trustees
- Blockchain records them
- Neff shuffle and decrypt



Talk Outline

- The appeal and history of E-voting
- **What's missing: key unsolved challenges**
  - **Keeping secrets off- or on-chain**
  - Transparency versus long-term privacy
  - Coercion and vote-buying
- Conclusion: there's promise, but be cautious

Talk Outline

- The appeal and history of E-voting
- **What's missing: key unsolved challenges**
  - Keeping secrets off- or on-chain
  - **Transparency versus long-term privacy**
  - Coercion and vote-buying
- Conclusion: there's promise, but be cautious

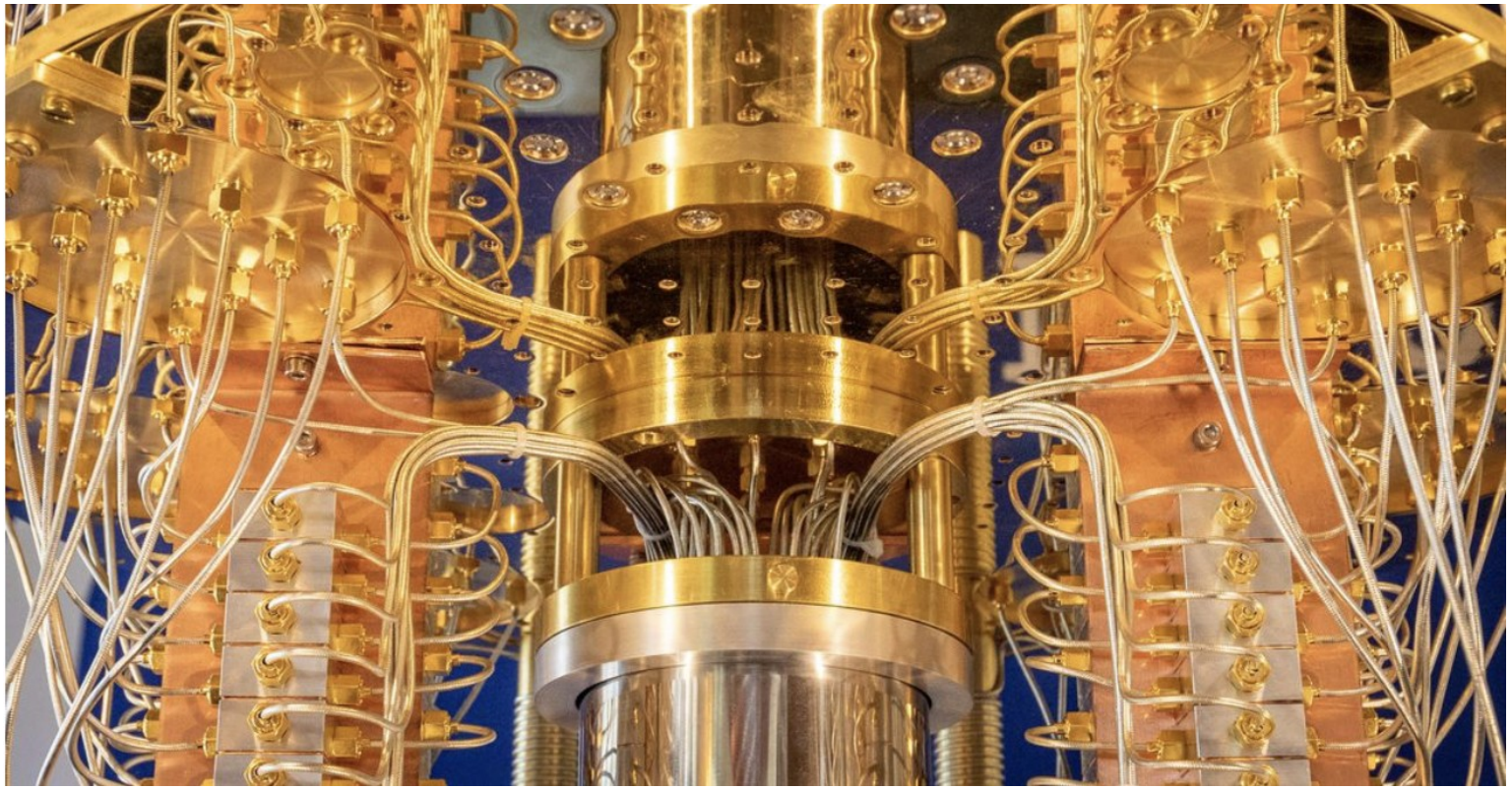
What about long-term privacy?

If today's encryption gets broken in 10 years, will your vote today be revealed to everyone?

Verifiability needs your encrypted vote public, but **long-term privacy** needs it not public.

What about long-term privacy?

Quantum computers may eventually break today's most flexible and verifiable encryption schemes



Post-quantum crypto is coming but not yet mature

E-voting with “Everlasting Privacy”

Research designs exist, but not yet deployed

Receipt-Free Universally-Verifiable Voting with Everlasting Privacy*

Coercion-Resistant Internet Voting with Everlasting Privacy

Philipp Locher[1,2], Rolf Haenni[1], and Reto E. Koenig[1]

[1] Bern University of Applied Sciences, CH-2501 Biel, Switzerland
{philipp.locher,rolf.haenni,reto.koenig}@bfh.ch
[2] University of Fribourg, CH-1700 Fribourg, Switzerland
philipp.locher@unifr.ch

Talk Outline

- The appeal and history of E-voting
- **What's missing: key unsolved challenges**
  - Keeping secrets off- or on-chain
  - **Transparency versus long-term privacy**
  - Coercion and vote-buying
- Conclusion: there's promise, but be cautious

Talk Outline

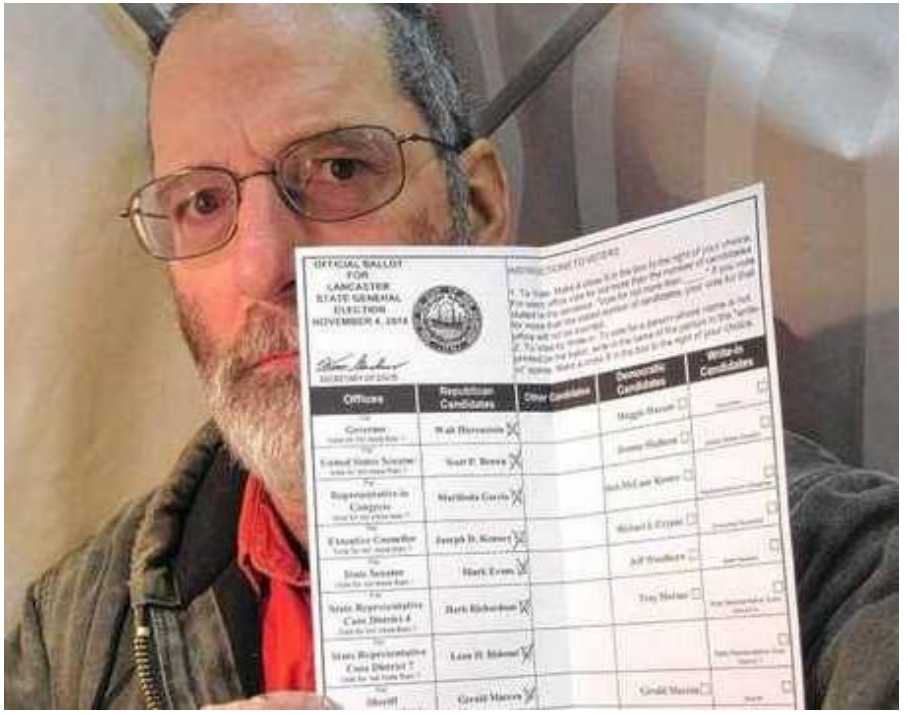
- The appeal and history of E-voting
- **What's missing: key unsolved challenges**
  - Keeping secrets off- or on-chain
  - Transparency versus long-term privacy
  - **Coercion and vote-buying**
- Conclusion: there's promise, but be cautious

Coercion and vote-buying

A potential threat affecting *all* voting methods…

- E-voting, postal voting, in-person voting

But risks are not equally *scalable* or *undetectable*



The New York Times

North Carolina Operative Indicted in Connection With Election Fraud

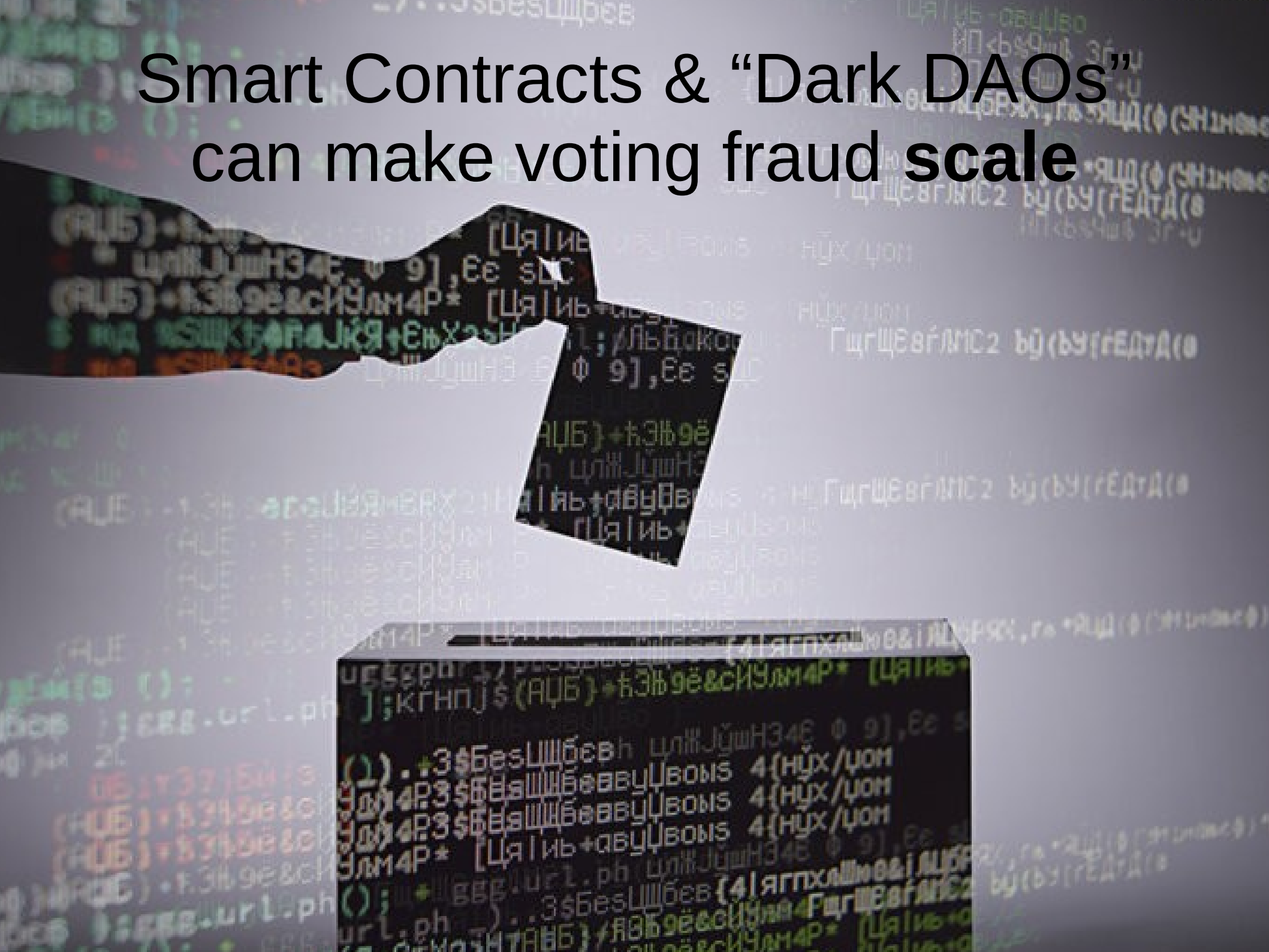
Yes, electoral fraud happens in Switzerland too

Despite a reputation for democratic exactitude, mishaps have sometimes affected Swiss votes in the past. For example, the **collection of signatures** for the deposition of a People's initiative (100,000 are necessary) can lead to forgeries, although the Federal Chancellery does its best to weed them out.

Elsewhere, some well-known examples in recent years include **Glarus**, where in 2010 a recount was ordered following the discovery that several ballots were filled-out by the same person. The result: the conservative right Swiss People's Party had to cede one of the seats it initially won.

In **Bern**, in 2016, 300 votes in local elections were declared void after investigators discovered they all had the same handwriting. And in **Valais**, the following year, 119 irregularities were found in three municipalities in an election that saw well-known politician Oscar Freysinger lose his seat. The margin of loss (2,000 votes) dissuaded his followers from pursuing the case.

Smart Contracts & “Dark DAOs” can make voting fraud **scale**



Hacking, Distributed

On-Chain Vote Buying and the Rise of Dark DAOs

on-chain voting voting e-voting trusted hardware identity selling ethereum

July 02, 2018 at 03:22 PM

Philip Daian, Tyler Kell, Ian Miers, and Ari Juels

Approaches to Coercion-Resistance

Estonia: a coerced voter can “re-vote” again later

- Critical flaw: coercion to vote at the last minute

Approaches to Coercion-Resistance

Decoy Ballots: fake ballots to give out or sell

- Problem: how to *obtain* decoy ballots safely?

Approaches to Coercion-Resistance

DEDIS Votegral framework: **https://votegral.org**

- Supports **E-voting**, **postal**, and **in-person** voting
  - Also **continuous participation**, e.g., liquid democracy
- Usable: **Easy** for voters to obtain decoy ballots
  - Give to your kids to play with and **learn** how to vote
  - Give to someone **coercing** you to vote their way
  - Sell them to anyone offering to **buy** your vote
- Entire E-voting pipeline **verifiable** end-to-end
  - All voters, credentials **transparent** on public ledger
  - Votes cast on one device are **checkable** on others

Talk Outline

- The appeal and history of E-voting
- **What's missing: key unsolved challenges**
  - Keeping secrets off- or on-chain
  - Transparency versus long-term privacy
  - **Coercion and vote-buying**
- Conclusion: there's promise, but be cautious

Talk Outline

- The appeal and history of E-voting
- What's missing: key unsolved challenges
  - Keeping secrets off- or on-chain
  - Transparency versus long-term privacy
  - Coercion and vote-buying
- **Conclusion: there's promise, but be cautious**

Conclusion

E-voting and Blockchain: yes it *can* work…

- Promises of convenience, online participation, transparency, end-to-end verifiability

But…

- “Blockchain” isn’t actually *new* in E-voting tech, and doesn’t solve *any* of the hardest problems
- Beware quick-to-market products without deep design review, vote privacy, coercion resistance

More: https://dedis.epfl.ch/ - https://votegral.org/