Are “blockchain” ideas useful in E-voting and E-governance?

Prof. Bryan Ford
Decentralized and Distributed Systems Lab
(DEDIS)

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

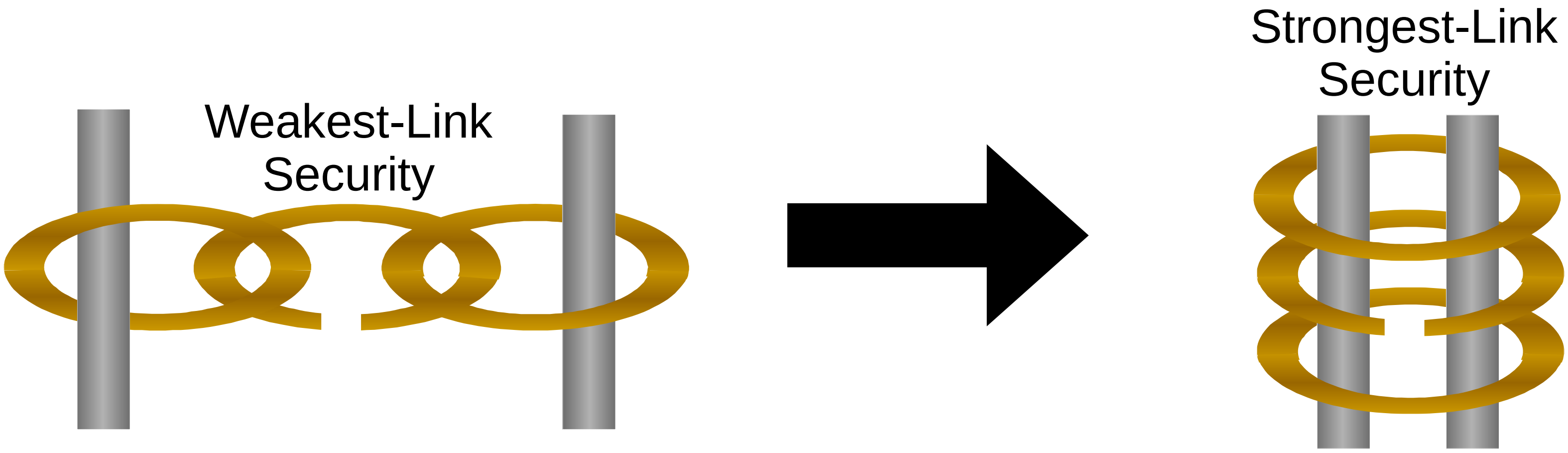
Federal Chancellery – September 20, 2017

The DEDIS lab at EPFL: Mission

Design, build, and deploy secure privacy-preserving
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*

Overarching theme: building decentralized systems
that **distribute trust** widely with **strongest-link security**



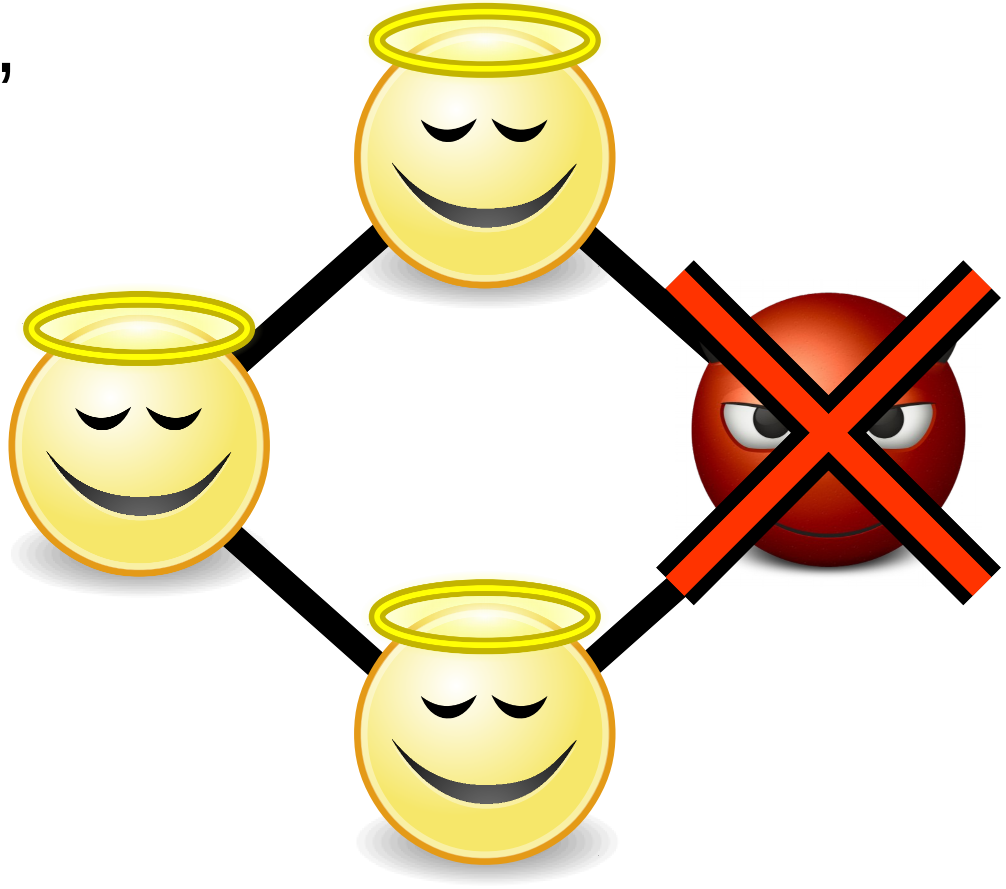
Blockchain and E-voting: Outline

- What is a Blockchain?
  - Why it’s exciting, what it’s good for, limitations
- Blockchain ideas we **DON’T** want in E-voting
- Blockchain ideas we **MIGHT** want in E-voting
- Conclusion

Decentralized Security Principles

Computer science theory, algorithms, crypto has long known *principles* of decentralized security…

- Threshold cryptography, Byzantine consensus
- Tolerate any one (or several) arbitrary failures or compromises



Decentralized Security Principles

Computer science theory, algorithms, crypto has long known *principles* of decentralized security…

- Threshold cryptography, Byzantine consensus
- Tolerate any one (or several) arbitrary failures or compromises

But never widely *deployed,* until…

Bitcoin (2008)

First successful decentralized cryptocurrency

Today’s Hot Decentralized Technology

(credit: Tony Arcieri)

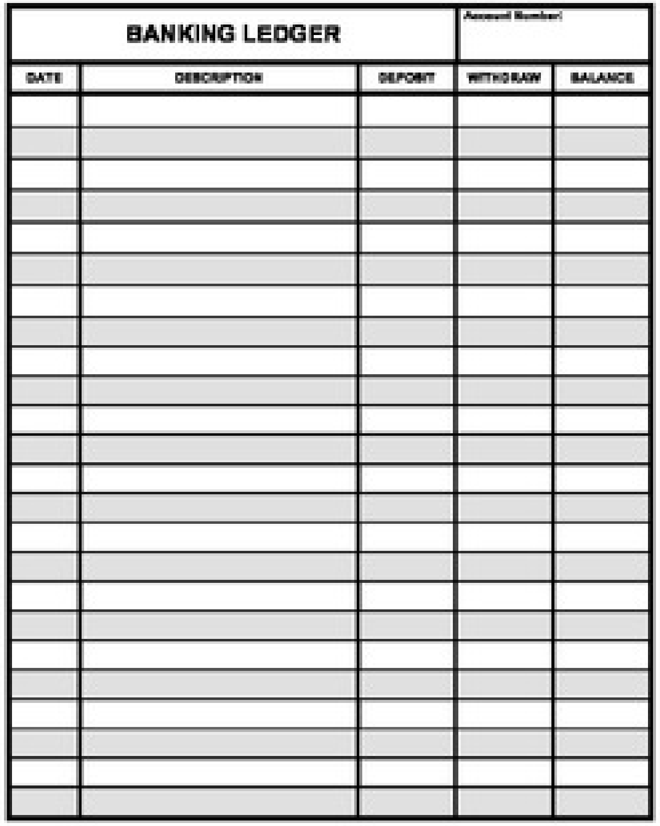
How to track wealth (or anything)?

Things

- Gold, beads, cash...

Ledgers

- Who owns what?



BANKING LEDGER

Account Number:

DATE	DESCRIPTION	DEPOSIT	WITHDRAW	BALANCE

Precedent: the Rai Stones of Yap

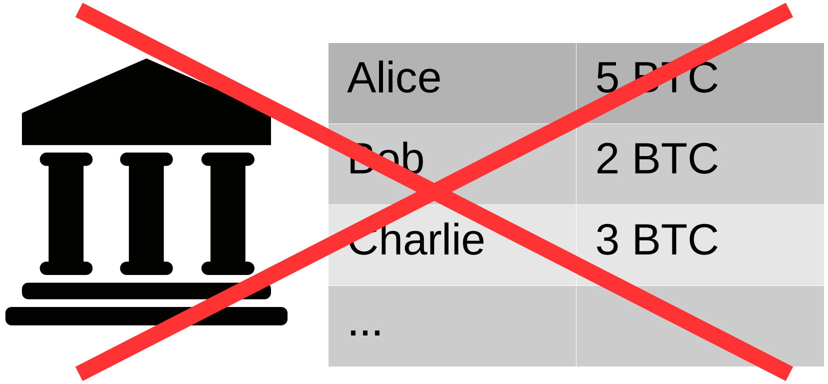
Stone “coins” weighing thousands of kilograms

- Left in place once created (“mined”)
- Ownership transfer by *public proclamation*

(this comparison shamelessly borrowed from Gün Sirer and others)

Distributed Ledgers

Problem: we don't want to trust any designated, centralized authority to maintain the ledger



Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Solution: “everyone” keeps a copy of the ledger!

- Everyone checks everyone else's changes to it

Alice's copy

Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Bob's copy

Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Charlie's copy

Alice	5 BTC
Bob	2 BTC
Charlie	3 BTC
...	

Applications of Distributed Ledgers

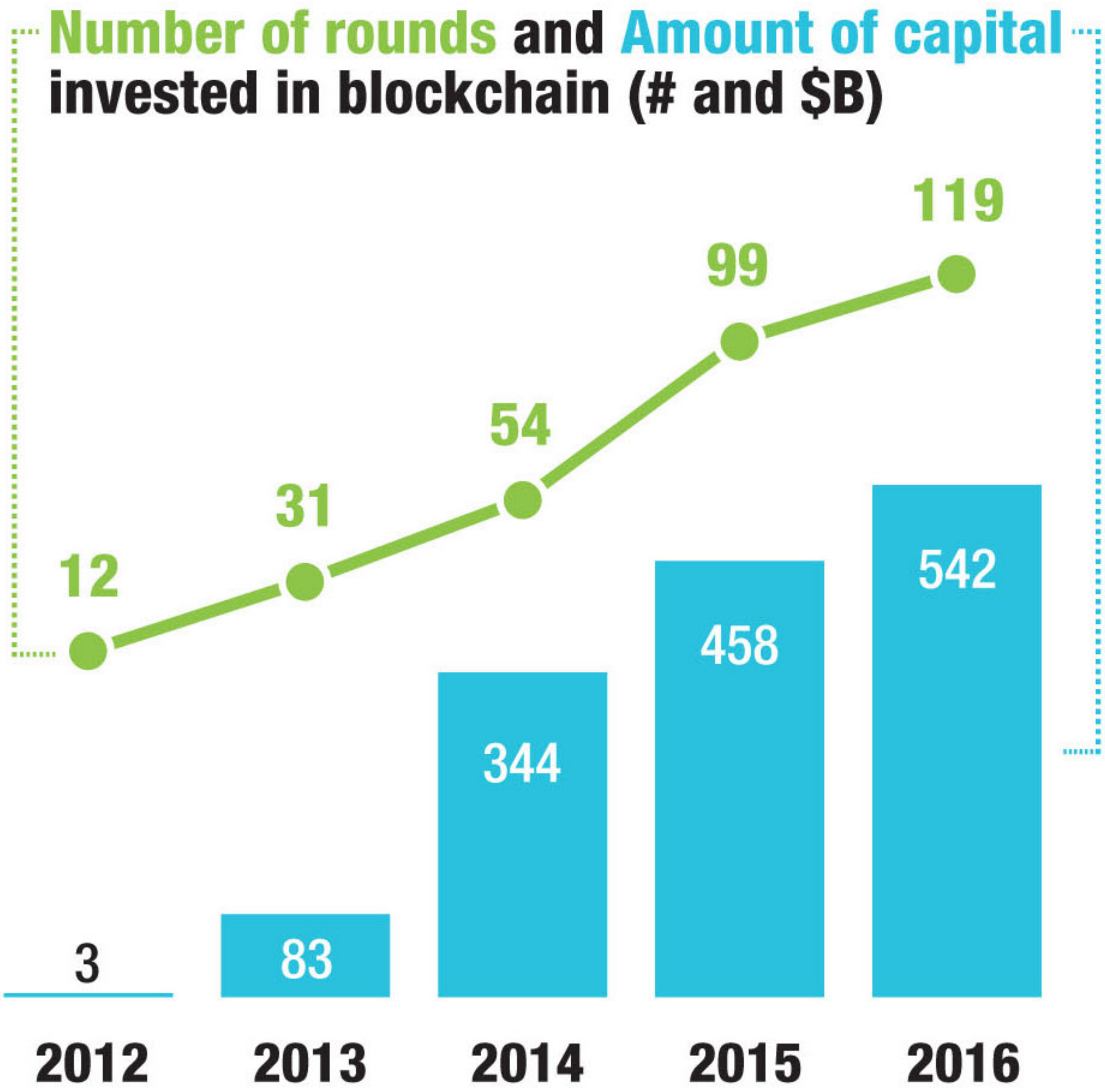
Can represent a distributed electronic record of:

- Who owns how much **currency**? (Bitcoin)
- Who owns a name or a digital work of art?
- What are the terms of a **contract**? (Ethereum)
- When was a **document** written? (notaries)

But practical limitations currently constrain uses

- Slow, energy-inefficient, can’t keep secrets…

Broad Promise & Global Interest



Source: Money of the Future, Life.SREDA

There is a **decreasing tendency towards launching new blockchain companies:**

2016	**169**
2015	**221**
2014	**233**

new companies launched

There is an **increase in investment rounds:**

2016	**119**
2015	**99**
2014	**54**

rounds

Limitations of Today’s Blockchains

Public/permissionless (e.g., Bitcoin, Ethereum)

- Slow, weak consistency, low total throughput
- Limited privacy: leaky, can’t keep secrets
- User devices must be online, well-connected
- Mining is inefficient, insecure, re-centralizing

Private/permissioned (e.g., HyperLedger, R3, …)

- Weak security – single points of compromise

Dimensions of Information Security

We usually want *three* orthogonal properties:

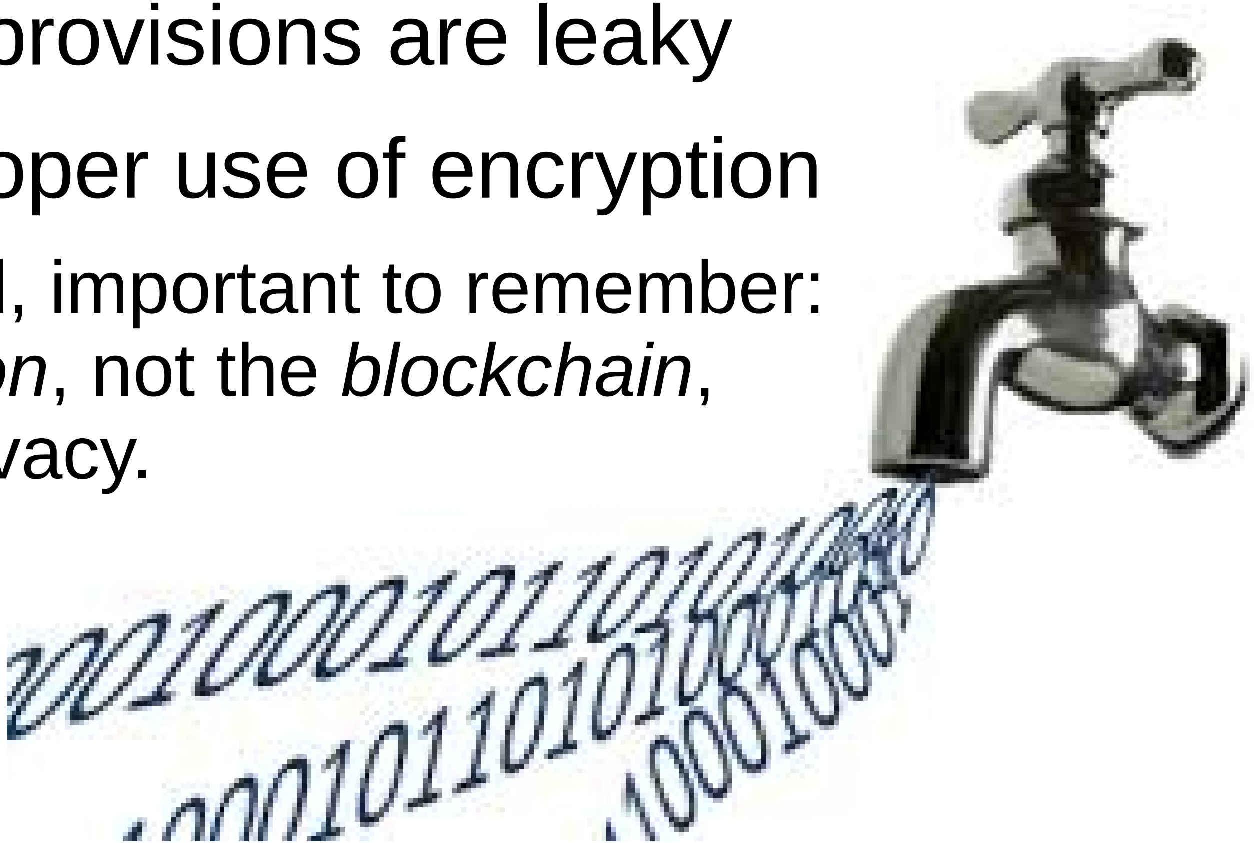
1. **Integrity:** the system computes honestly, remembers and results correctly
2. **Availability:** it’s there when you need it, provides answers in reasonable amount of time
3. **Privacy:** it doesn’t leak confidential information to anyone who isn’t supposed to have it

In general, blockchains tend to be
GOOD at #1, SO-SO at #2, and BAD at #3

The Blockchain Privacy Challenge

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

- This works *against* **privacy** & confidentiality
- Current privacy provisions are leaky
- Solvable with proper use of encryption
  - When combined, important to remember: it’s the *encryption*, not the *blockchain*, that protects privacy.



Blockchain and E-voting: Outline

- What is a Blockchain?
  - Why it’s exciting, what it’s good for, limitations
- **Blockchain ideas we DON’T want in E-voting**
- Blockchain ideas we **MIGHT** want in E-voting
- Conclusion

Blockchain E-voting: The Bad

Blockchain ideas we **DON’T** want in E-voting:

- Proof-of-Work (or Proof-of-Stake or…)
  - Energy waste, don’t want open consensus group
- Nakamoto Consensus
  - Slow, only probabilistically secure over time
- General-purpose Smart Contracts (Ethereum)
  - Huge systemic risks from subtle contract bugs

Proof-of-Work in Public Blockchains

Public blockchains such as Bitcoin, Ethereum use consensus by crypto-lottery

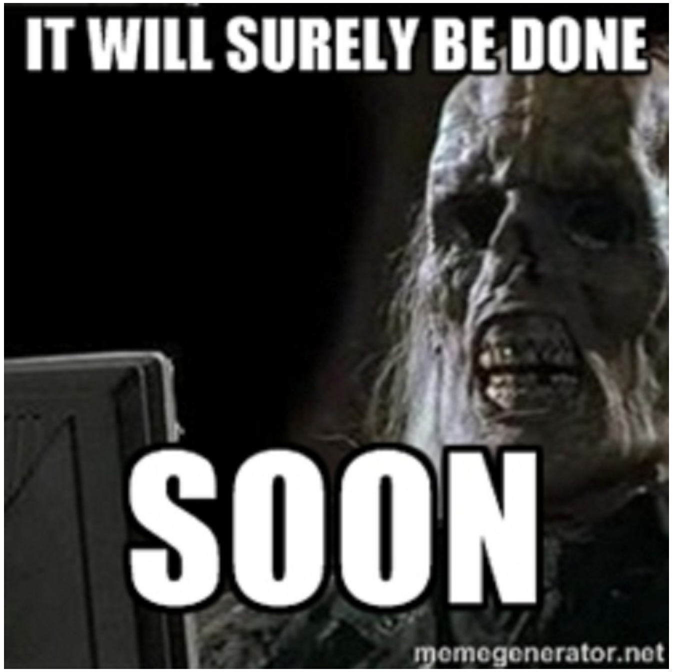
1) **Miners** print their own “lottery tickets” by solving crypto-puzzle (**proof-of-work**)

2) Winner gets to add one **block** to blockchain; typically gets **reward**: e.g., print new money

3) All miners gravitate to **longest chain.** Repeat.

Drawbacks of Nakamoto Consensus

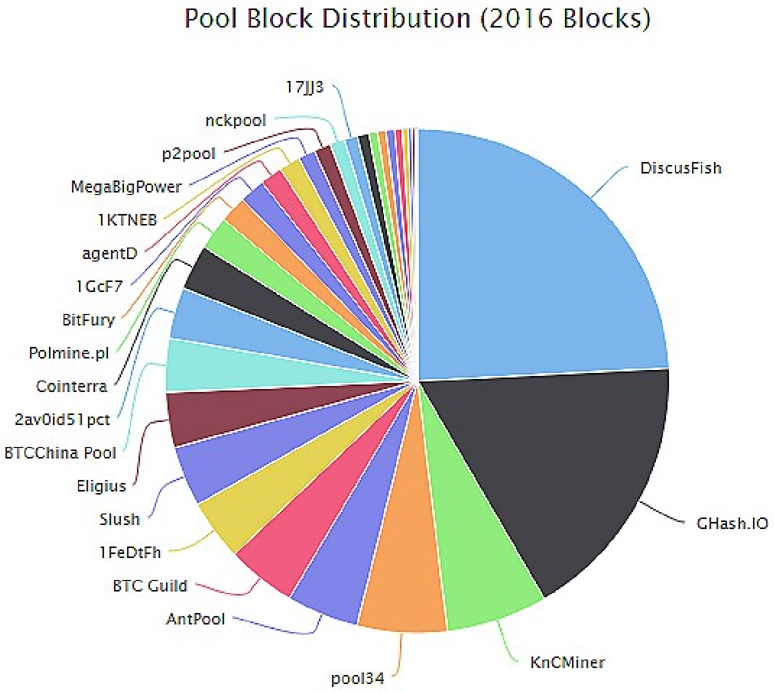
- **Transaction delay**
  - Any transaction takes ~10 mins *minimum* in Bitcoin
- **Weak consistency:**
  - You’re not *really* certain your transaction is committed until you wait ~1 hour or more
- **Low throughput:**
  - Bitcoin: ~7 transactions/second
- **Proof-of-work mining:**
  - Wastes huge amount of energy



Who Participates in Consensus?

Permissionless blockchains (Bitcoin, Ethereum): “anyone” who invests in solving crypto-puzzles.

- Now practical only with ASICs and cheap power
- Re-centralization undermines trustworthiness



Environmental Costs

Proof-of-work = “scorched-earth” blockchains

- Tremendous energy waste,
  now comparable to all of Ireland

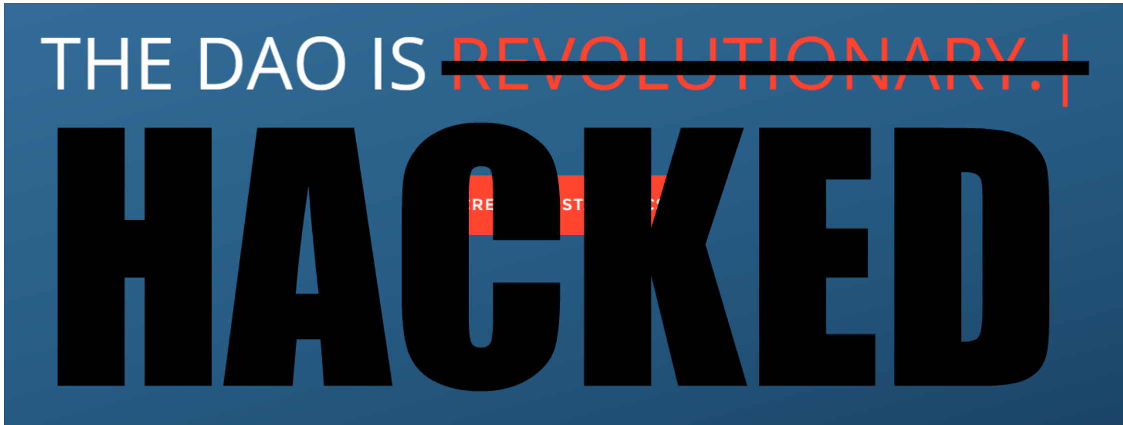
Smart Contracts (e.g., Ethereum)

Insert arbitrary *software* into a blockchain

- Can programmatically supervise cryptocurrency
  - e.g., automatically settle a financial contract

Extremely powerful (and interesting), but risky

- One software bug → spectacular hacks
  - DAO: $70M USD of $150M USD contract stolen in hours (June 2016)



Blockchain and E-voting: Outline

- What is a Blockchain?
  - Why it’s exciting, what it’s good for, limitations
- Blockchain ideas we **DON’T** want in E-voting
- **Blockchain ideas we MAY want in E-voting**
- Conclusion

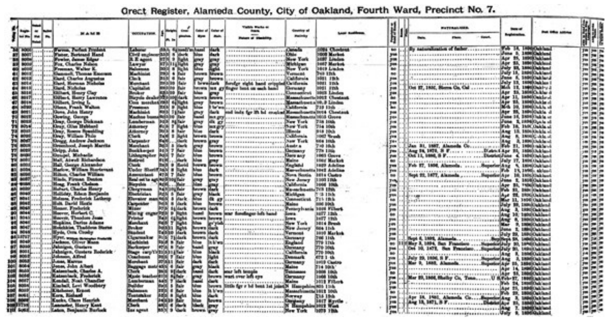
Blockchain E-voting: The Good

Blockchain ideas we **MIGHT** want in E-voting:

- Tamper-evident publicly-verifiable ledger
- Open protocols, standards, software
- Strong security hardening incentives
- Trust splitting (threshold security)
- Cross-layer implementation diversity
- Sharing costs through common platforms
- “Not-too-smart” contracts enabling innovation

Elements of E-Voting

- Voter registration
- Vote casting and recording
- Results tallying and certification

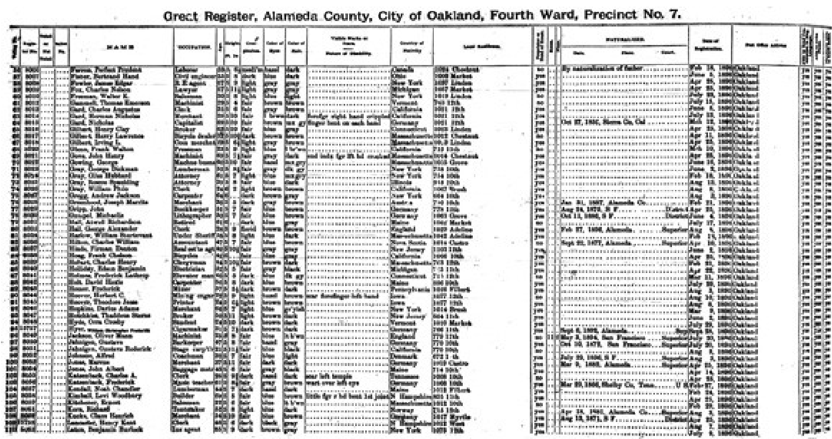


Great Register, Alameda County, City of Oakland, Fourth Ward, Precinct No. 7.

Potential Uses in Voter Registration

- Enable individual voters to check their own registration easily (e.g., online, any time)
- Enable everyone to sanity-check total counts
  - Do all those registered voters really exist?
    Guard against large-scale registration fraud risks
- Transparency in linking registration to identity, online democracy, other government services

Challenges: voter privacy,
small-scale fraud, …



Great Register, Alameda County, City of Oakland, Fourth Ward, Precinct No. 7.

Potential Uses in Voting

Many E-voting systems put encrypted and shuffled votes on a public “bulletin board”

- A blockchain can be a good bulletin board

Final results need to be publicly “certified”

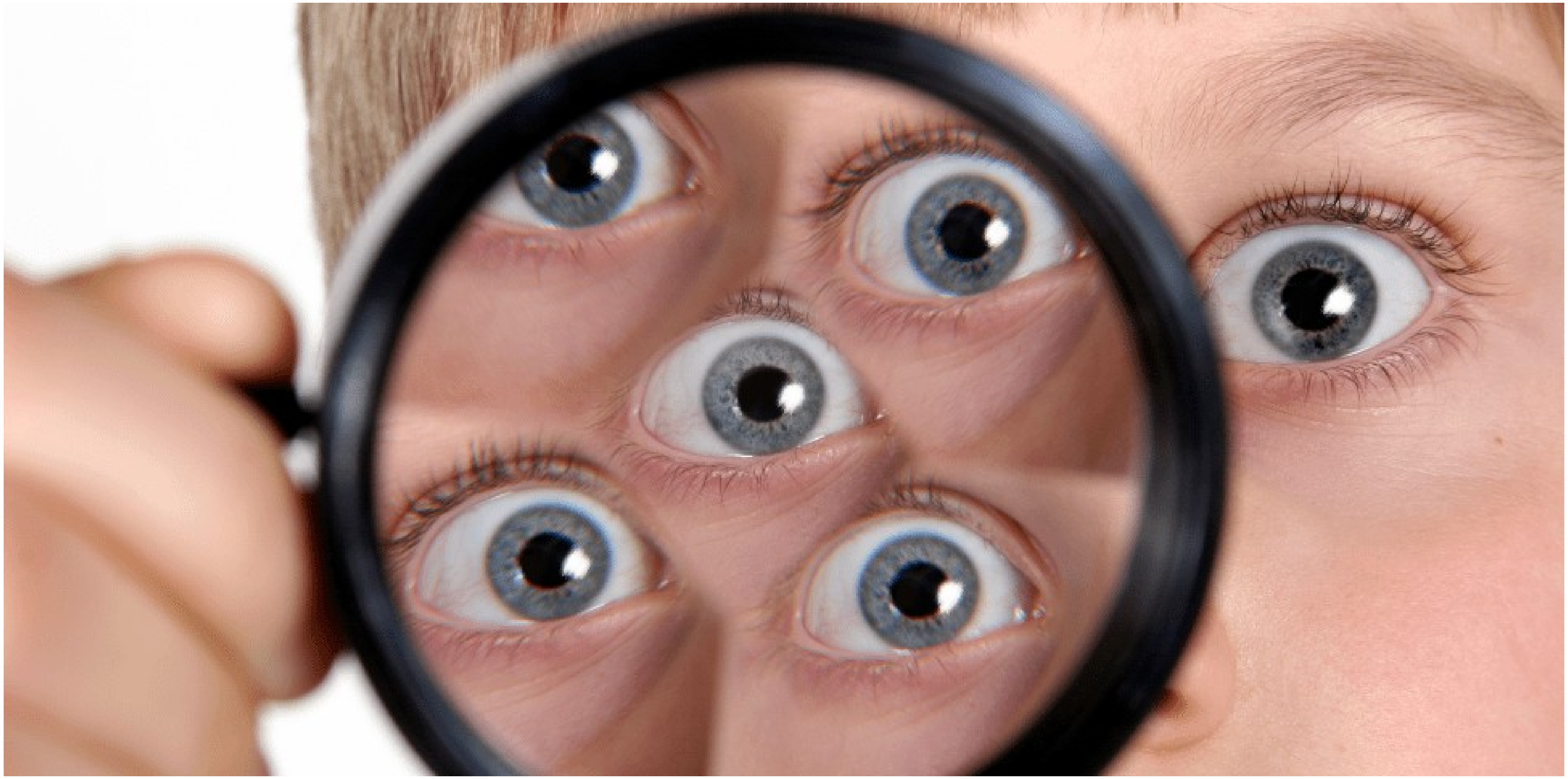
- Put [hash of] final results on public blockchain to ensure everyone sees & agrees on results

Blockchain *doesn’t* help with integrity or privacy of casting, encryption, or shuffling votes: need crypto

Potential Benefits of Openness

Open protocols, specifications, software

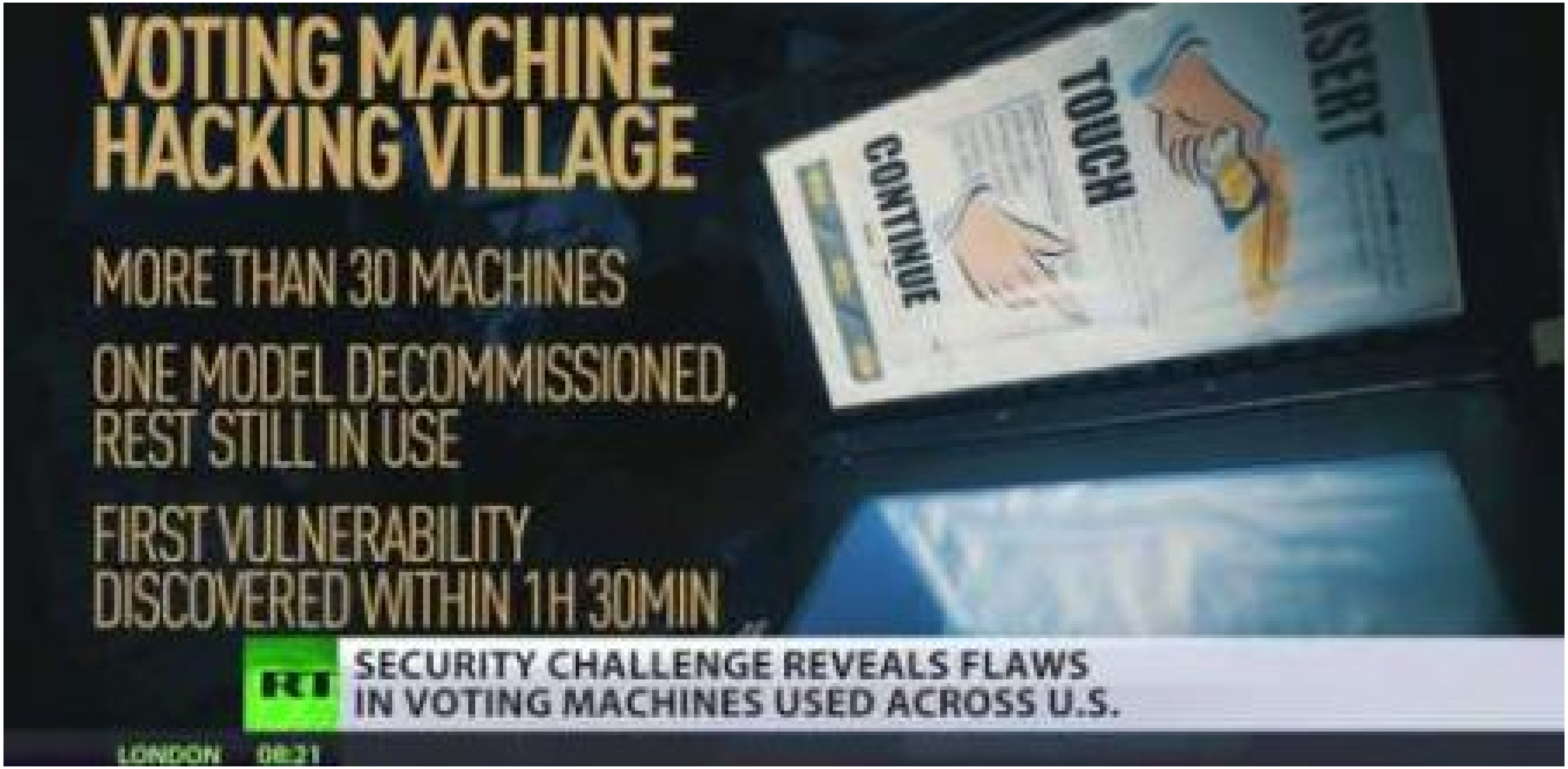
- Security benefits from scrutiny of “many eyes”



DEFCON 17 Hacking Village

Security through obscurity doesn’t work anymore

- Hackers’ patience, tools, resources too good



VOTING MACHINE HACKING VILLAGE

MORE THAN 30 MACHINES

ONE MODEL DECOMMISSIONED, REST STILL IN USE

FIRST VULNERABILITY DISCOVERED WITHIN 1H 30MIN

SECURITY CHALLENGE REVEALS FLAWS IN VOTING MACHINES USED ACROSS U.S.

Security Hardening Incentives

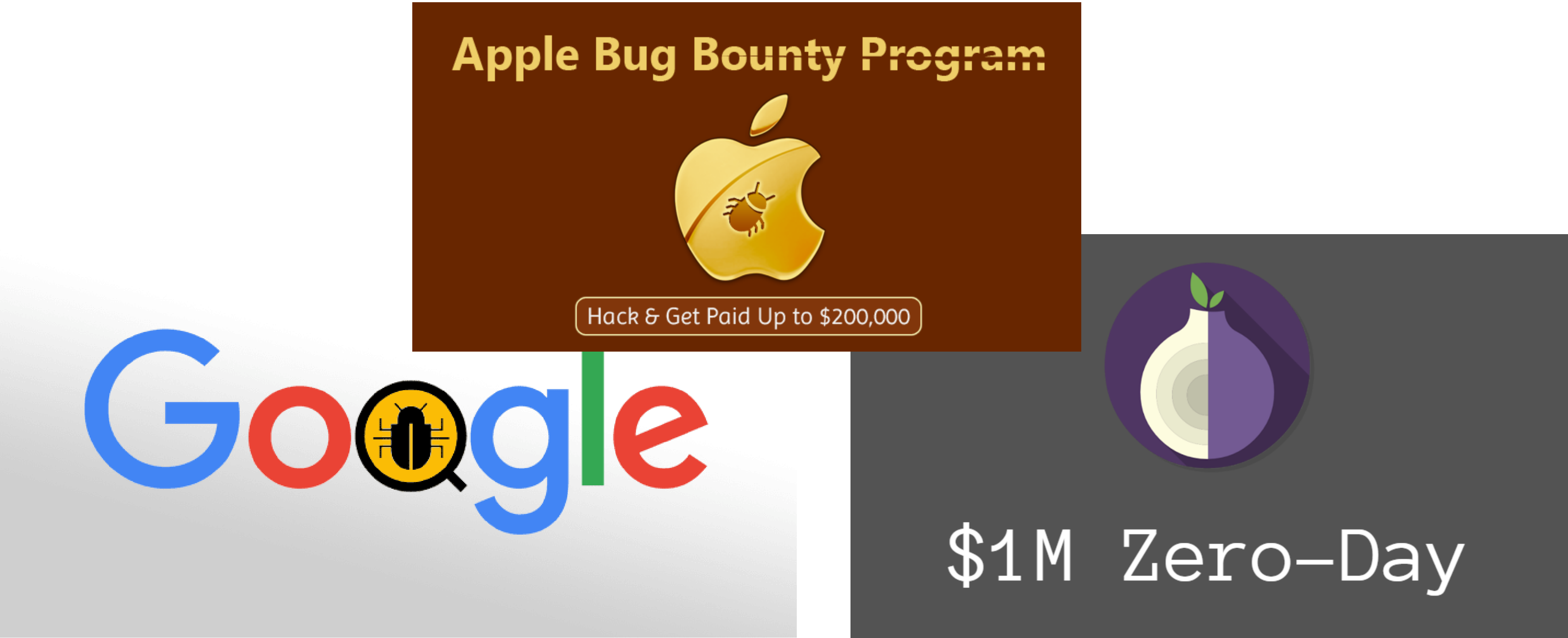
Bitcoin, Ethereum are “universal bug bounties”

- First successful hacker can steal a *lot* of money

Security Hardening Incentives

We don’t need or want to embed a cryptocurrency into an E-voting/governance system…

But robust *bug bounty* programs can substitute

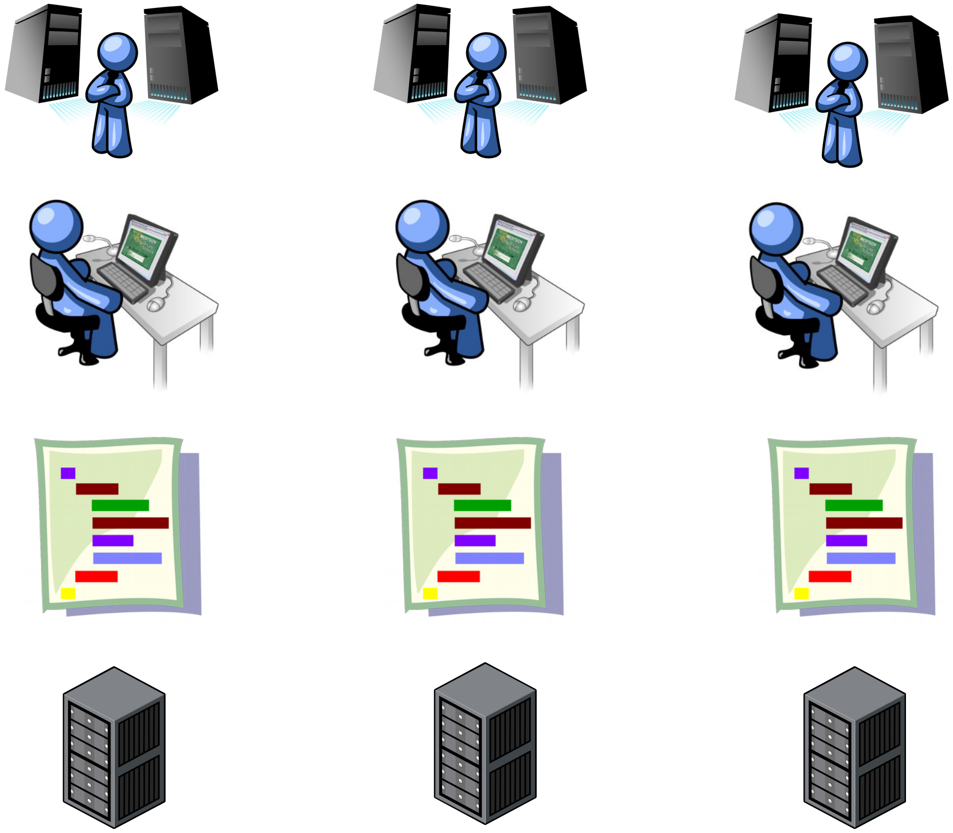


Trust Splitting (Threshold Security)

Avoid single points of failure, compromise

But risks come at many levels…

- Operators
- Developers
- Software
- Hardware



The Diversity Challenge

Trust-splitting is ineffective without *diversity*

- If all Bitcoin nodes run by the same operator, compromised miner → blockchain-wide breach
- If all Bitcoin nodes run exact same software, one software bug → blockchain-wide breach
- If different software but identical hardware, one hardware bug → blockchain-wide breach

Importance of Cross-Layer Diversity

Robust blockchains (e.g., Bitcoin) have:

- Multiple independent *operators* (“miners”)
- Multiple independent *software implementations*
  - Bitcoin clients in C++, Java, Go, …
  - Written by different teams of developers
- Multiple independent *hardware platforms*
  - Run on Intel, AMD, ARM, …
  - Designed & built by different companies

Secure E-voting systems need this diversity too

Approaches to Achieving Diversity

“N-version” design

- Build 2,3,4 of everything
- Different teams, common specs

Disadvantage

- Expensive!
- Spec bugs
- Groupthink

Leader/verifier design

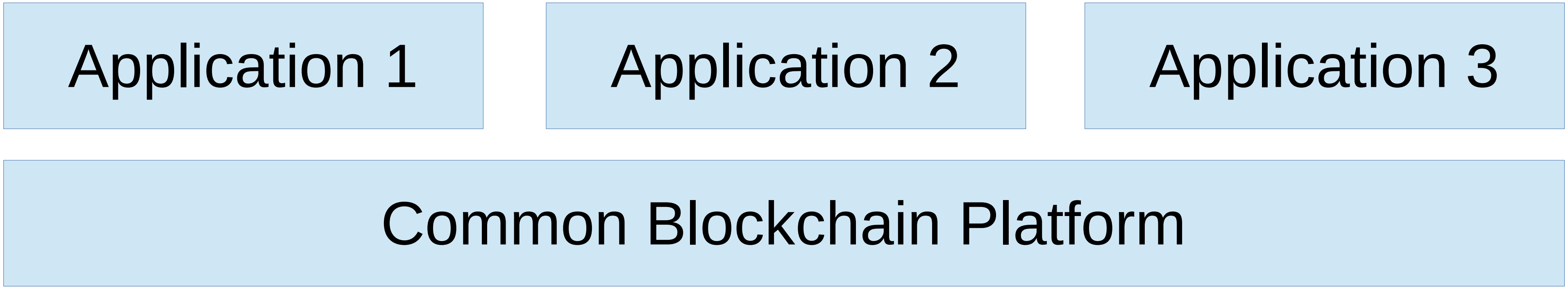
- Design & primary implementation from one team/company
- Other teams build minimal *verifiers*
  - Smaller, simpler
  - Cryptographically ensure leader cannot maliciously cheat

Sharing Costs through Platforms

Blockchain systems are becoming *platforms*

- Foundation layers usable by many applications
  - Not specific to cryptocurrencies, trading, E-voting…
- Development, security, and diversity costs of platform shared across multiple industries

E-voting could also benefit from platform sharing



Application 1

Application 2

Application 3

Common Blockchain Platform

“Not-Too-Smart” Contracts

Smart contracts (Ethereum) are a powerful idea

Could be useful and safe in voting systems
if adopted cautiously with *appropriate restrictions*

- Programmable via carefully-designed *domain-specific* languages for voting systems
  - *Simple:* to ensure behavior matches intent
  - *Safe:* automatically enforce properties like fairness
  - *Formal:* to allow automated reasoning, verification
- Promising and important, but research needed

Enabling E-Governance Innovation

Example: **Delegative** or **Liquid Democracy**

- Give users a *choice* to participate directly or via representative on a given topic

Direct + Representative = Delegative Democracy

Promising but nontrivial: **transparency** is crucial

- Blockchain-based implementation could help ensure transparency, public acceptance

Blockchain and E-voting: Conclusion

- Blockchains aren’t “The Answer”, but do hold important ideas for E-voting system designs
  - Ledger concept useful in registration, vote recording
  - Openness, incentives can help harden security
  - Trust-splitting: a critical tool, but requires diversity
- Adoption requires care in both tech and policy