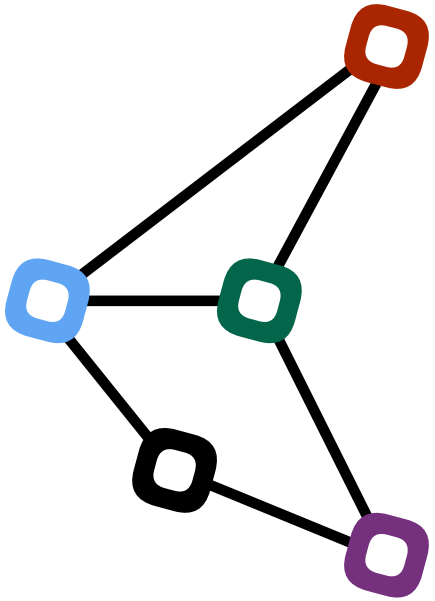
EPFL dedis



Decentralized and Distributed Systems Laboratory (DEDIS)

Prof. Bryan Ford
dedis@epfl.ch – dedis.epfl.ch

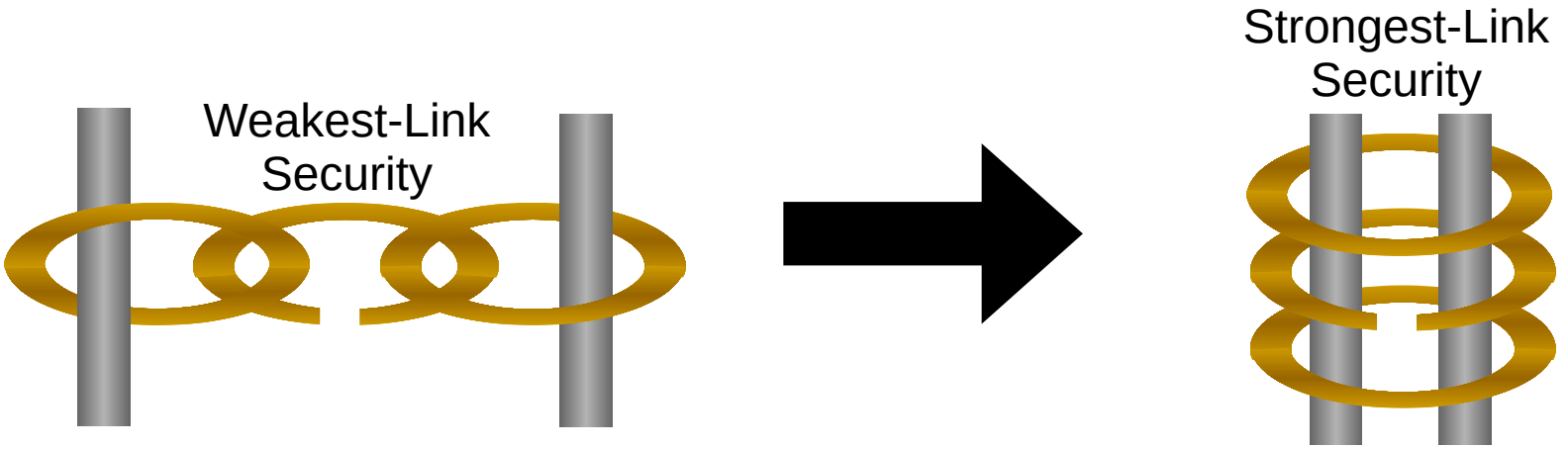
EDIC Research Seminars – September 2, 2025

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*

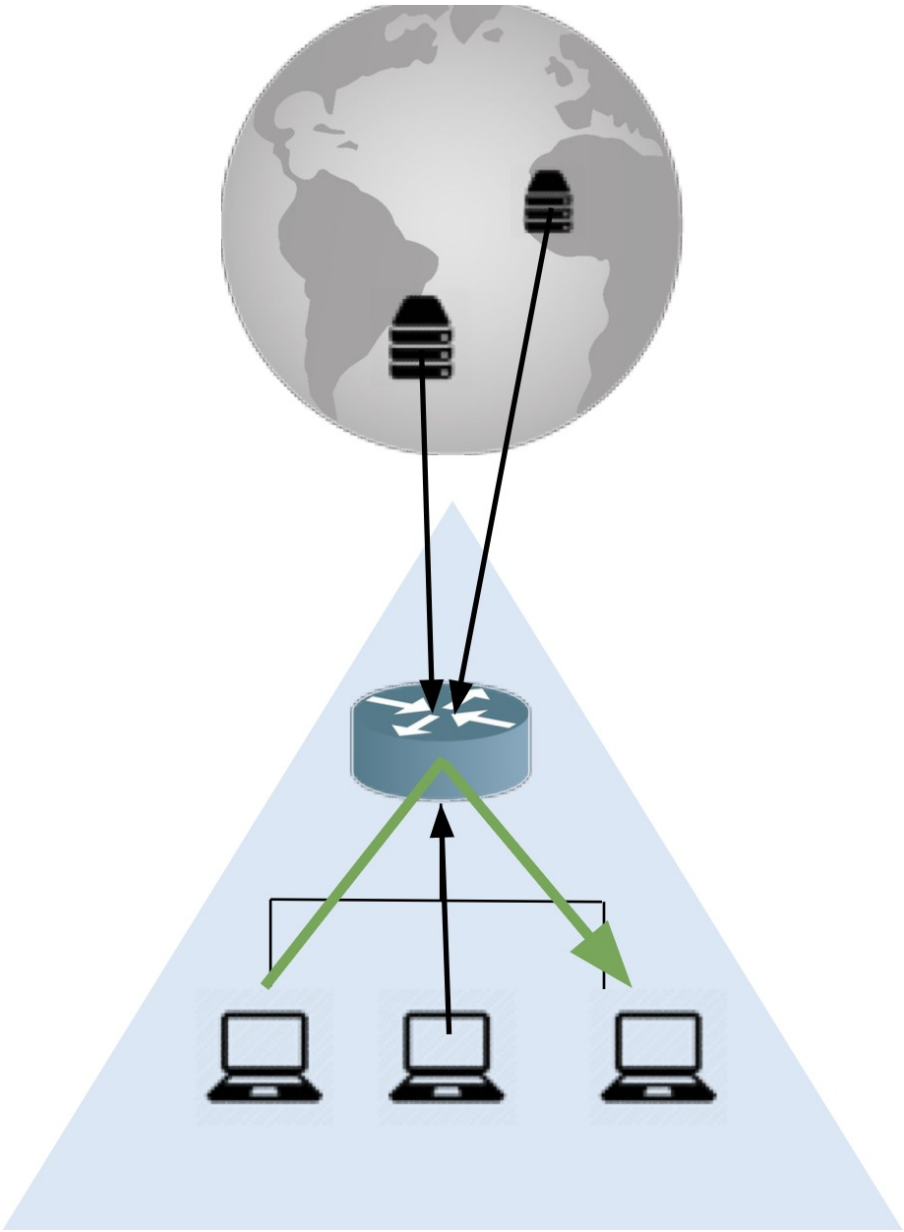
Overarching theme: building decentralized systems
that **distribute trust** widely with **strongest-link security**



PriFi: strong campus-area anonymity

Based on **DC-nets**
(**dining cryptographers)**

- But low latency:
  “one hop” up and down
  - No serial (onion) routing!
- Accountability against disruption or abuse

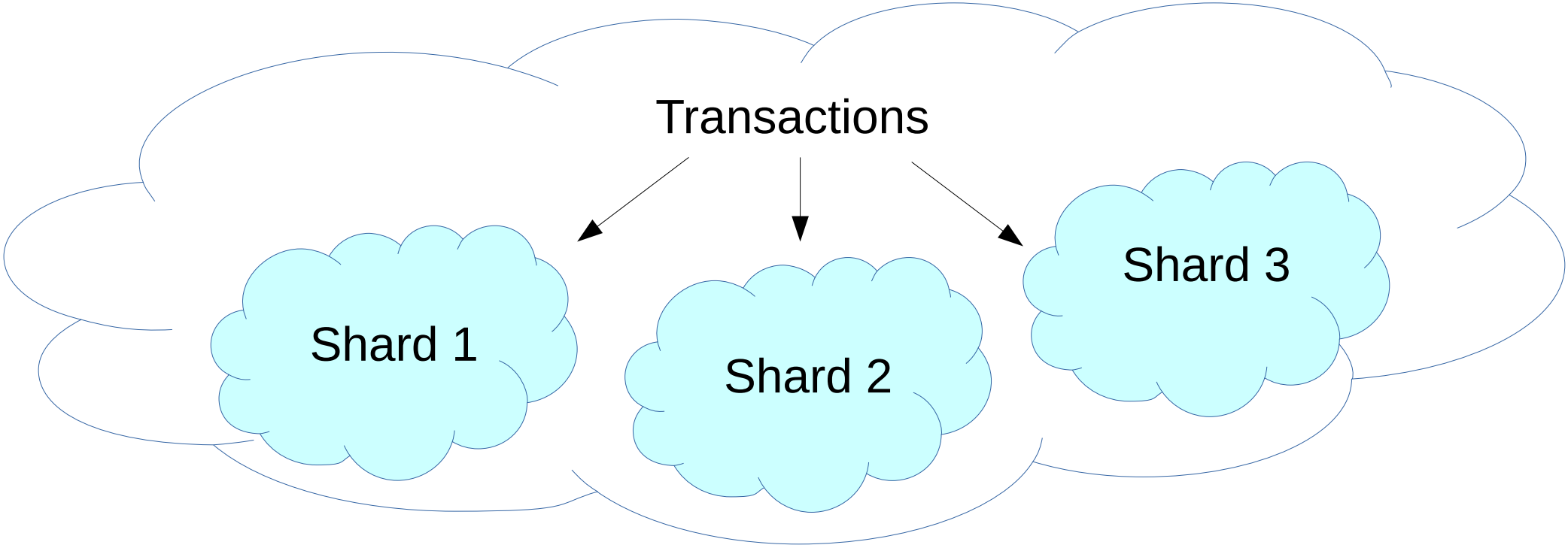


(credit: Tony Arcieri)

Horizontal Scaling via Sharding

OmniLedger: A Secure Scale-Out Ledger [S&P 18]

- Break large collective into smaller subgroups
- Builds on scalable bias-resistant randomness protocol (IEEE S&P 2017)
- 6000 transactions/second: competitive with VISA

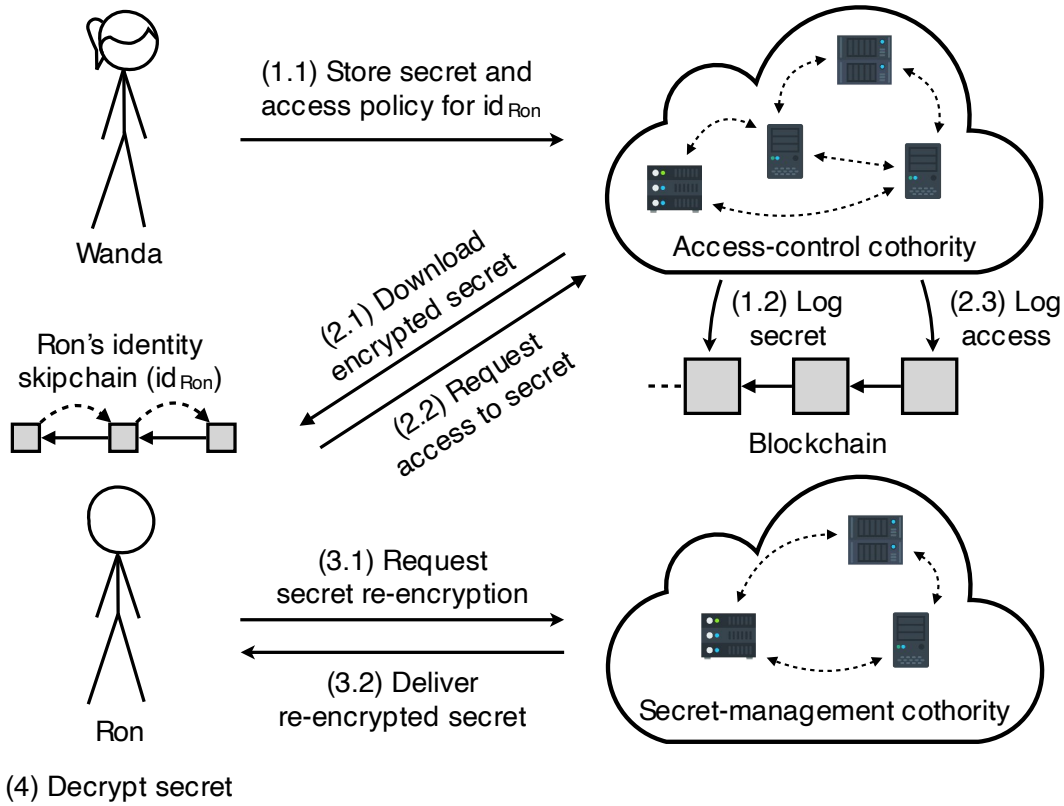


On-Chain Secrets

“CALYPSO: Private Data Management for Decentralized Ledgers” [VLDB ‘21]

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

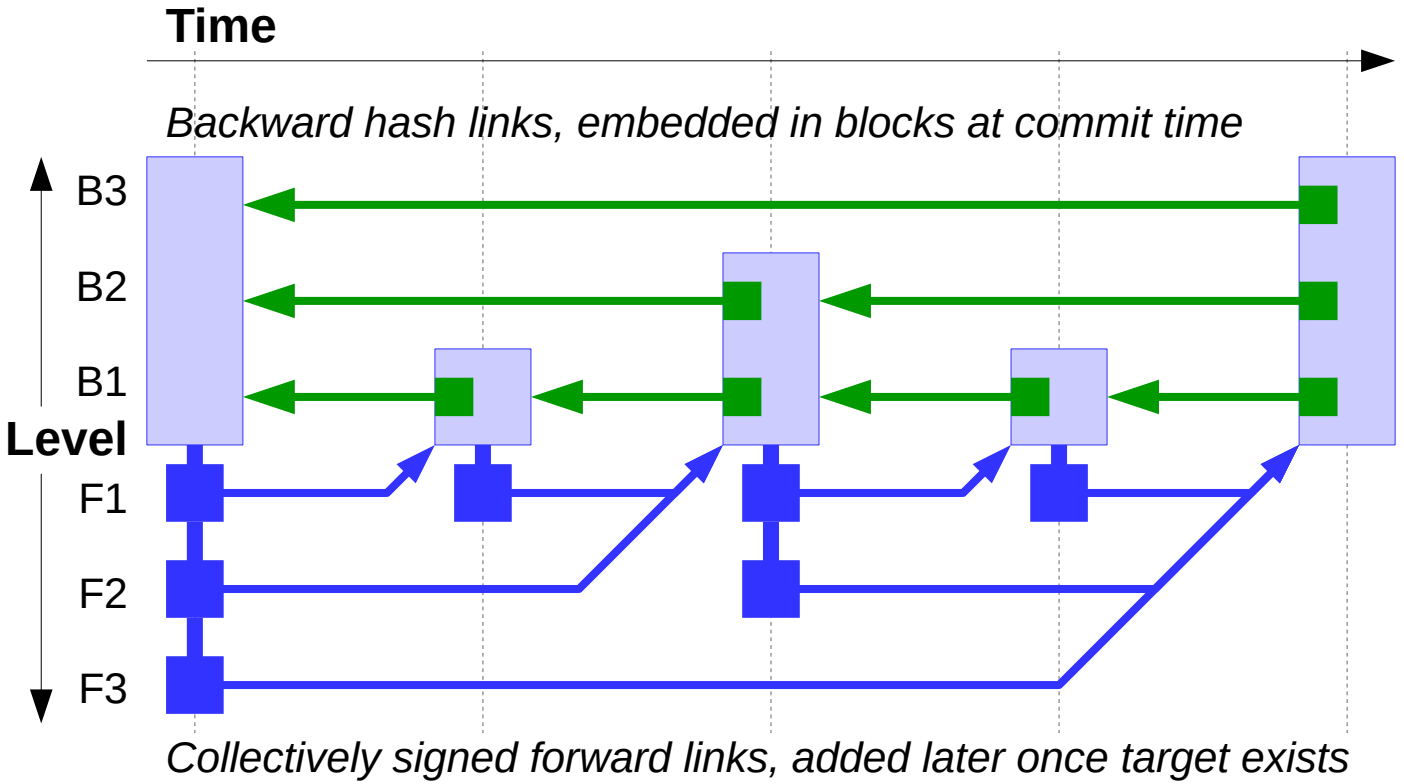
- Threshold of trustees mediate all accesses
- Enforce policies, access recording
- Ensure data both *hidden* and *disclosed* when policy requires
- Can *revoke* access if policy/ACLs change



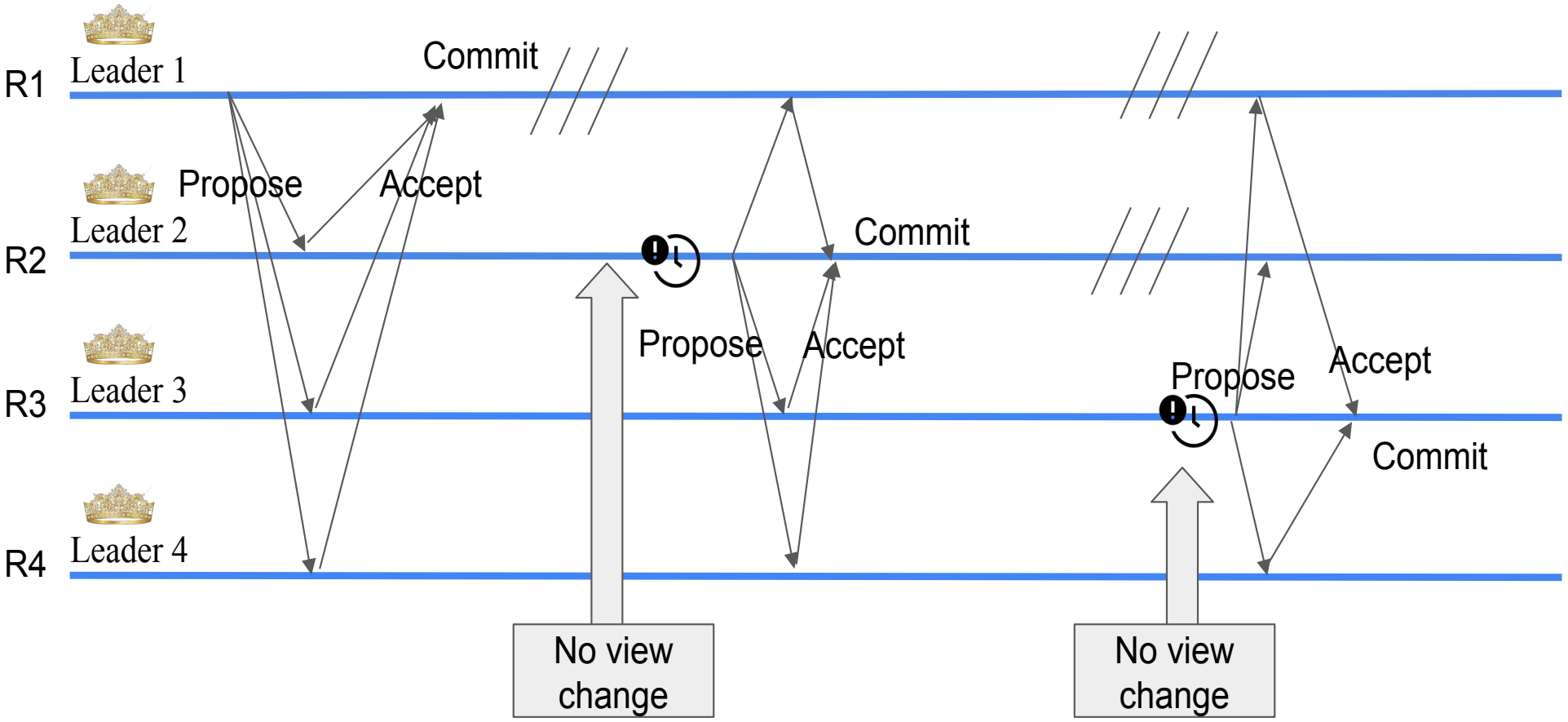
(*) with post-quantum security if desired

Leaping Through Time: SkipChains

Enables offline/peer-to-peer cryptographic verification and efficient “time-travel” through all blockchain history



QuePaxa: efficient consensus without view changes or timeouts



Common-case performance, efficiency of Paxos/Raft
Worst-case robustness of asynchronous consensus

Decentralized Digital Democracy

Will decentralized online systems ever be able to **self-govern** in an egalitarian, democratic fashion?

[Kenneth Hacker, The Progressive Post]

The Coercion, Vote-Buying Problem

How can we know people vote their **true intent** if we can't secure the environment they vote in?

The Coercion, Vote-Buying Problem

Both **Postal** and **Internet** voting are vulnerable!

The New York Times

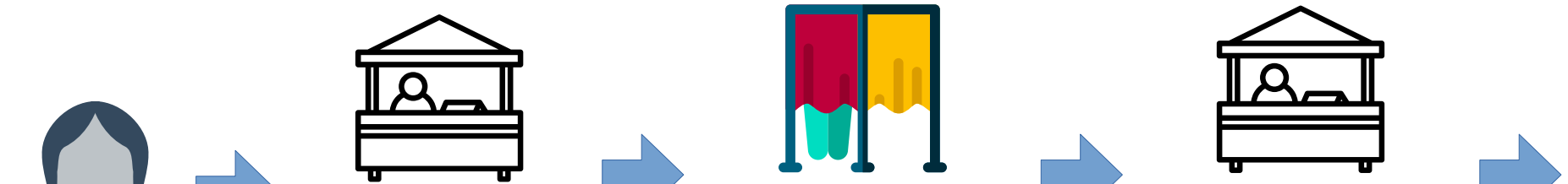
Election Fraud in North Carolina Leads to New Charges for Republican Operative

July 30, 2019

TRIP: Coercion-Resistant E-voting

Voter periodically registers/renews *in person*

- Gets verifiable *real* and *fake* credentials
- Fake credentials cast votes that *don't count*
- Voter learns difference (in privacy booth) but *can't prove it to anyone*



Check in
prove identity
get ticket

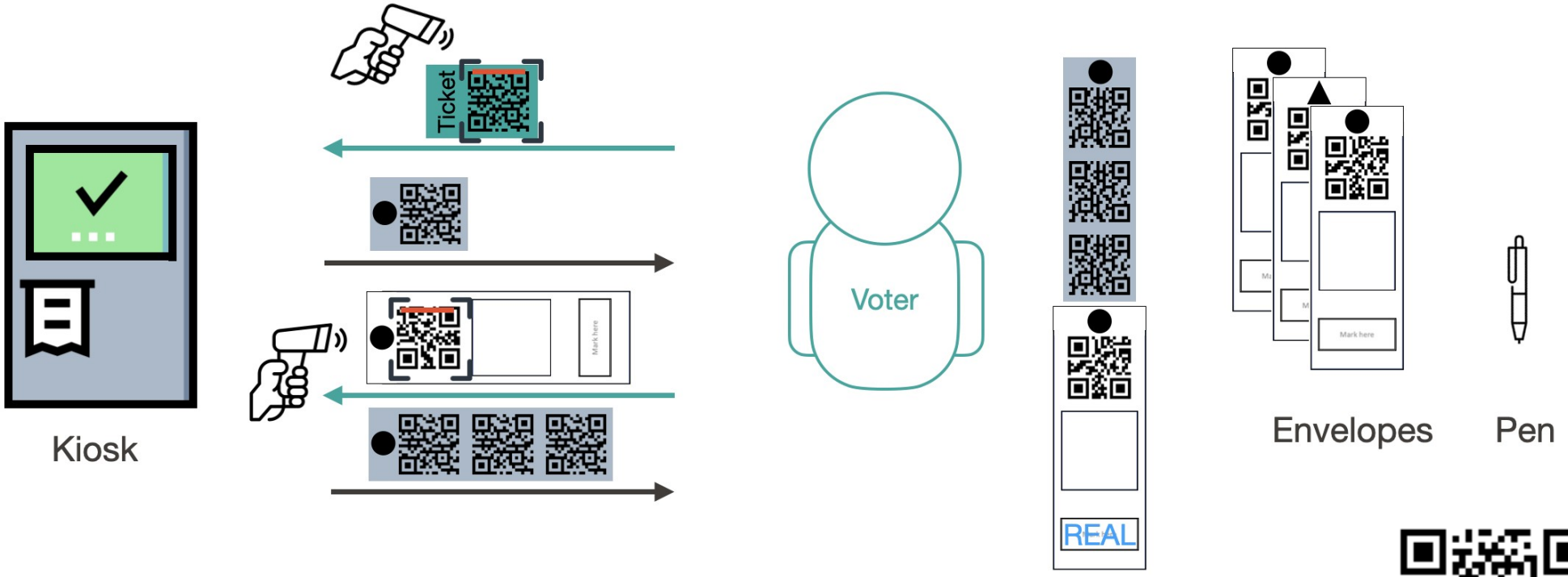
In private
get real, fake
credentials

Check out
show *any*
credential

In the booth: **real** credentials

Voters follow a 4-step process

- Unknowingly create a **sound** ZK proof

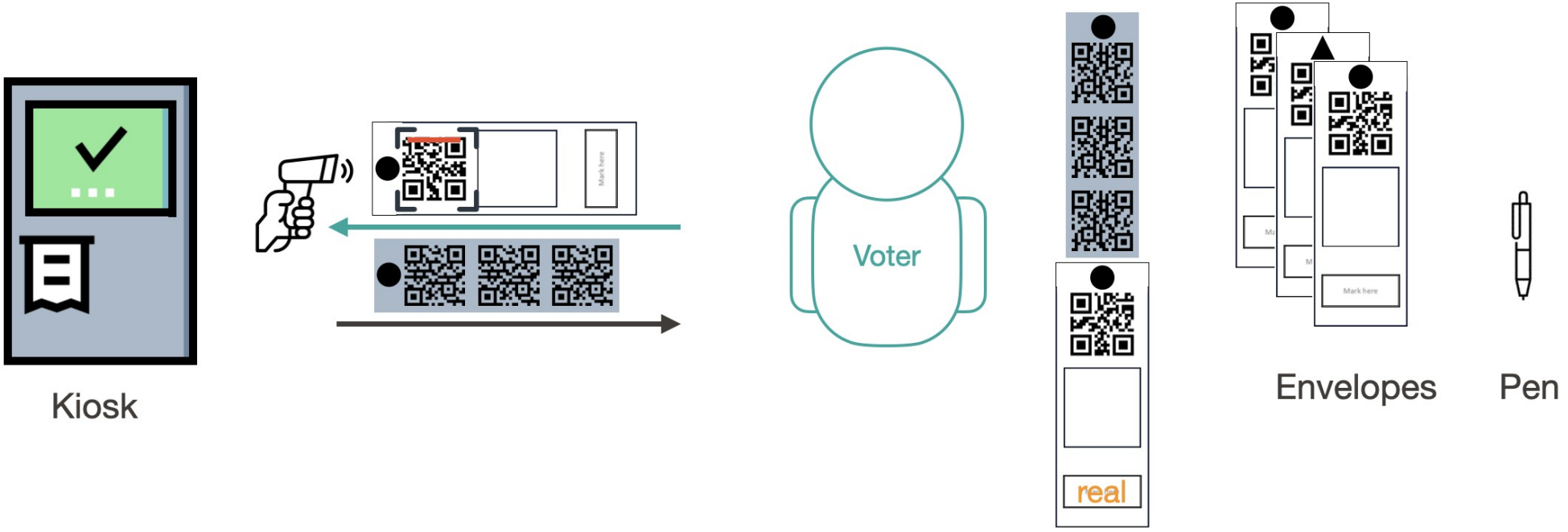


Usability study: **normal people can do this**

In the booth: **fake** credentials

Voters follow a distinct 2-step process

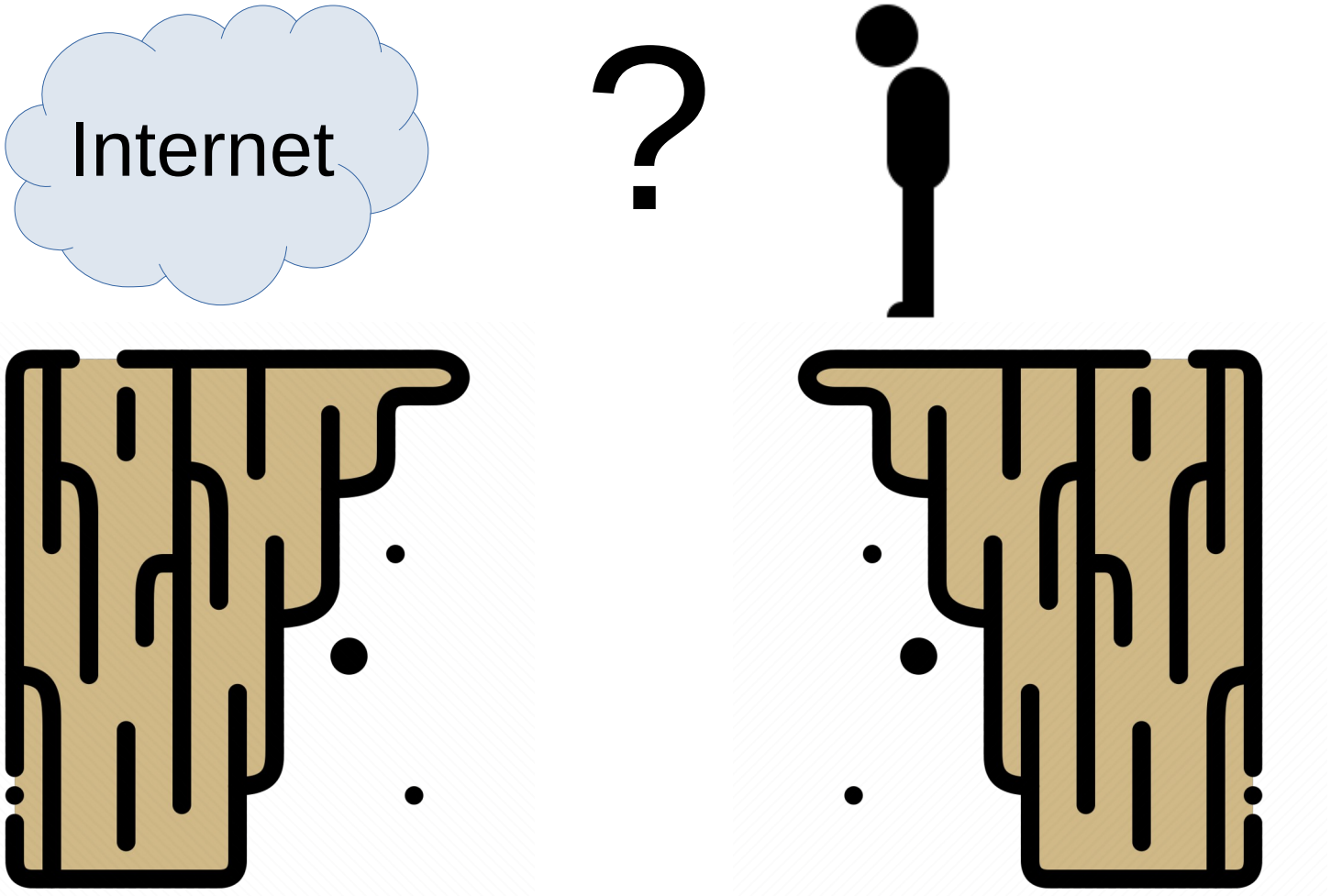
- Unknowingly create an **unsound** ZK proof



Voter knows which is real, but **can't prove it**

Proof of personhood (PoP)

How to authenticate a “**real person**” online?



Towards rich online participation

[Ehud Shapiro, Open Transcripts]

And now for something completely different…

Reasoning around paradox with grounded deduction

Do we have freedom of expression?

Casual programming

YES

main() { printf(“Hi!”); }

main() { main(); }

permissionless

Formal logic, verification

NO

“Show me your permit!”

permissioned

“Can we do *this* interesting thing”?

Casual programming

Formal logic, verification

“Not allowed!”

Gödel’s incompleteness theorem

What if…

…these symptoms are related?

The Liar Paradox

“This sentence is false”

$$L \equiv \neg L$$

The Liar Paradox

“This sentence is false” $L \equiv \neg L$

L false (hypothesis)

¬*L* false (*L*’s definition)

L true (negation)

L true (conclusion)

L true (hypothesis)

¬*L* true (*L*’s definition)

L false (negation)

L false (conclusion)

The Liar Paradox

“This sentence is false” $L \equiv \neg L$

Classical deduction

“Not allowed!”

Recursion must be justified

“Show me your permit!”

A (new?) reasoning principle

habeas quid

We must *have a thing* in order to use it.

~~Classical~~ proof by contradiction

Grounded

a bool

habeas quid

$$\frac{\begin{array}{c} a \text{ false} \\ \vdots \\ a \text{ true} \end{array}}{a \text{ true}}$$

The Liar Paradox

“This sentence is false” $L \equiv \neg L$

Classical deduction

“Not allowed!”

Recursion must be justified

“Show me your permit!”

Grounded deduction

Valid recursive definition

But is *L* a (bool) thing?

- To use contradiction, *first* prove *L* boolean

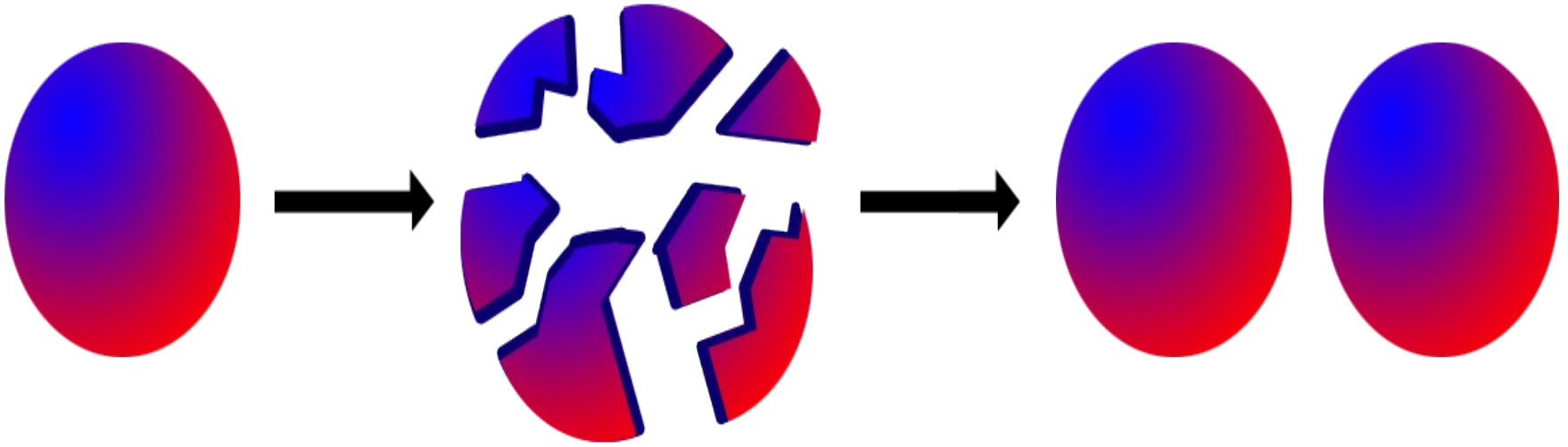
Curry's Paradox

"If this sentence is true then pigs fly" $C \equiv C \rightarrow P$

Classical/intuitionistic	**Grounded deduction**
Illegal circular definition!	Valid recursive definition
If allowed, inconsistency	But is *C* boolean?
• With only $\rightarrow I$ and $\rightarrow E$ (no classical LEM)	• To introduce $C \rightarrow P$, *first* prove *C* boolean

The Banach-Tarski Paradox

Set-theoretically reassemble 1 unit ball into 2



Uses Axiom of Choice – but maybe wrong culprit?

[image credit: cognitive coitus]

Grounded Arithmetic (GA)

Like Peano or Heyting arithmetic, but grounded

- **Computation-equivalent** formal reasoning
- PCL-like base plus **computable quantifiers**

Provably consistent: formalized in Isabelle/HOL

- Gödel's 1st incompleteness theorem: **trivial**
- Gödel's 2nd incompleteness theorem: **fails**
- Models own semantics, proves self consistent

Future work: **useful** grounded formal reasoning!

DEDIS lab research summary

Decentralized and distributed systems:

- Privacy and anonymity technologies
- Blockchains and cryptocurrencies
- Digital identity, personhood, and democracy
- …and crazy stuff, e.g., new logic foundations

dedis

Bryan Ford