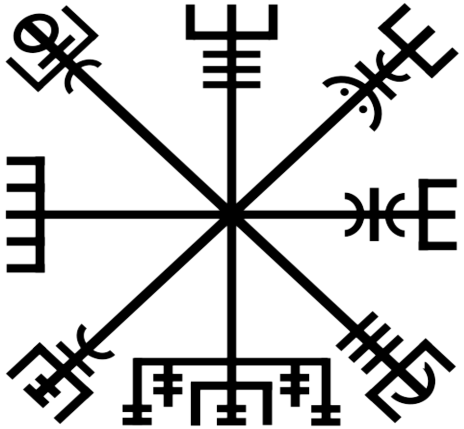
Emergency Edge Supercloud



Robbert van Renesse
Hakim Weatherspoon
Stephen Wicker
Danny Adams
Gloire Burambiza
Xinwen Wang

Cornell University

DISCLAIMER

This presentation was produced by guest speaker(s) and presented at the National Institute of Standards and Technology's 2019 Public Safety Broadband Stakeholder Meeting. The contents of this presentation do not necessarily reflect the views or policies of the National Institute of Standards and Technology or the U.S. Government.

Posted with permission

Motivation

- The 2017 Atlantic Hurricane Season was deadly and destructive
- Hundreds of lives were lost
- Over a quarter trillion dollars in estimated damages

Emergency First Responders

Loss of lives, limbs, and property would have been a lot higher if not for the efforts of thousands of first responders

Problem: communication infrastructure might not be available

- Cell towers rendered inoperable
- First responders can use only equipment they bring with them

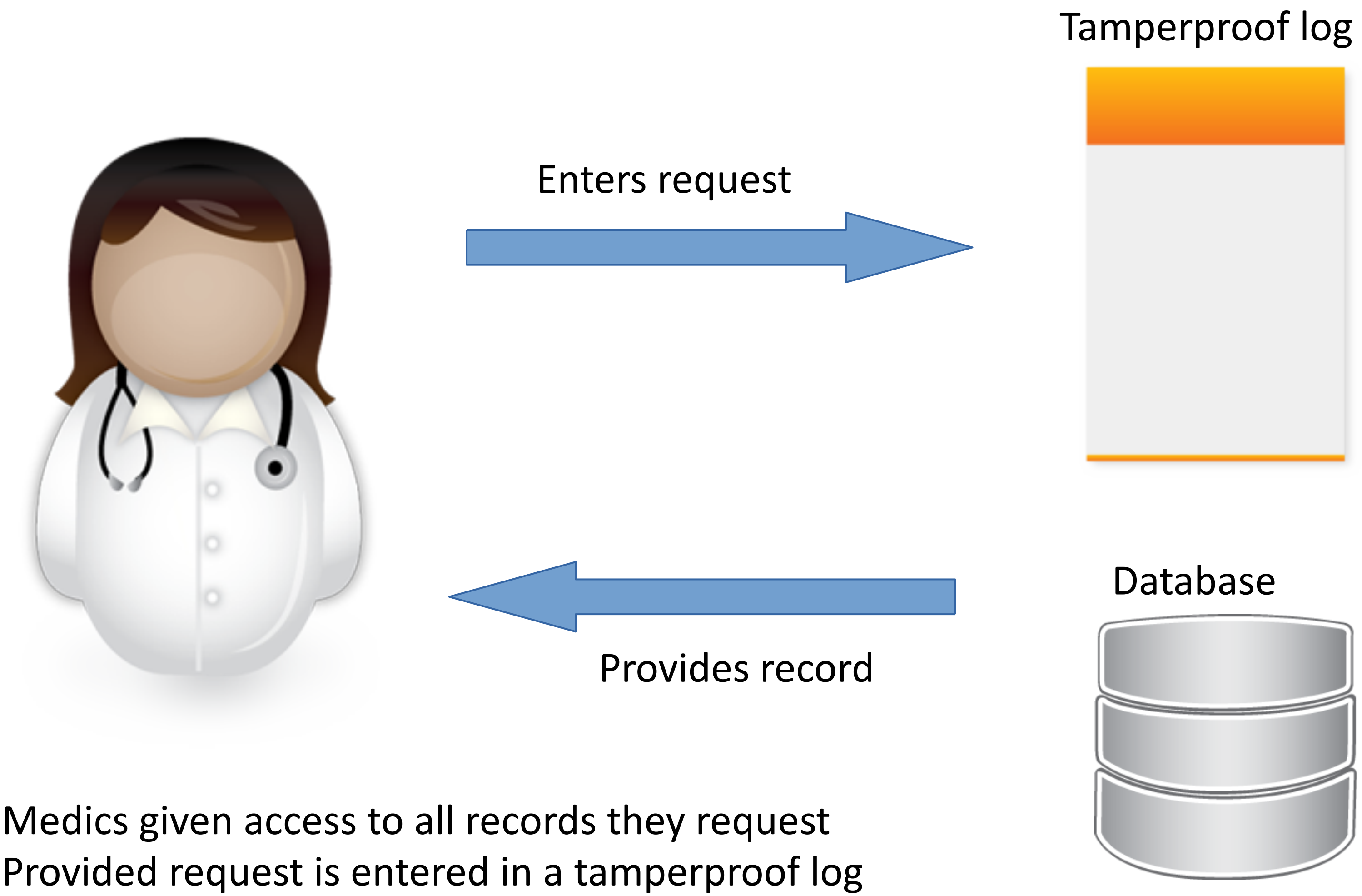
Opportunity: every first responder is carrying a computer and network router

- Smartphones come with a variety of communication modalities
- Can form ad-hoc networks

Prompt and privacy aware access to medical records

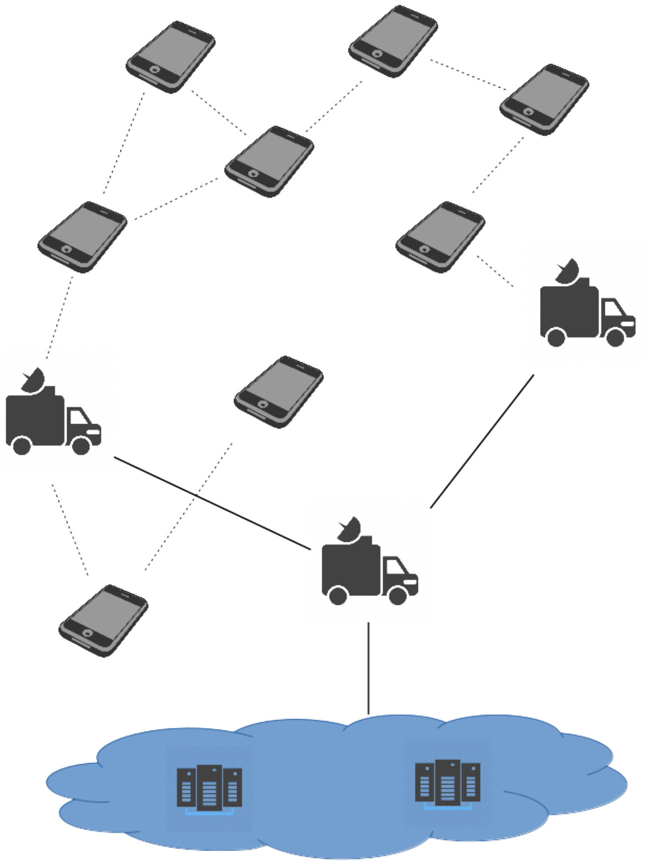
Problem: loss of communication with central server

Accountability over access control



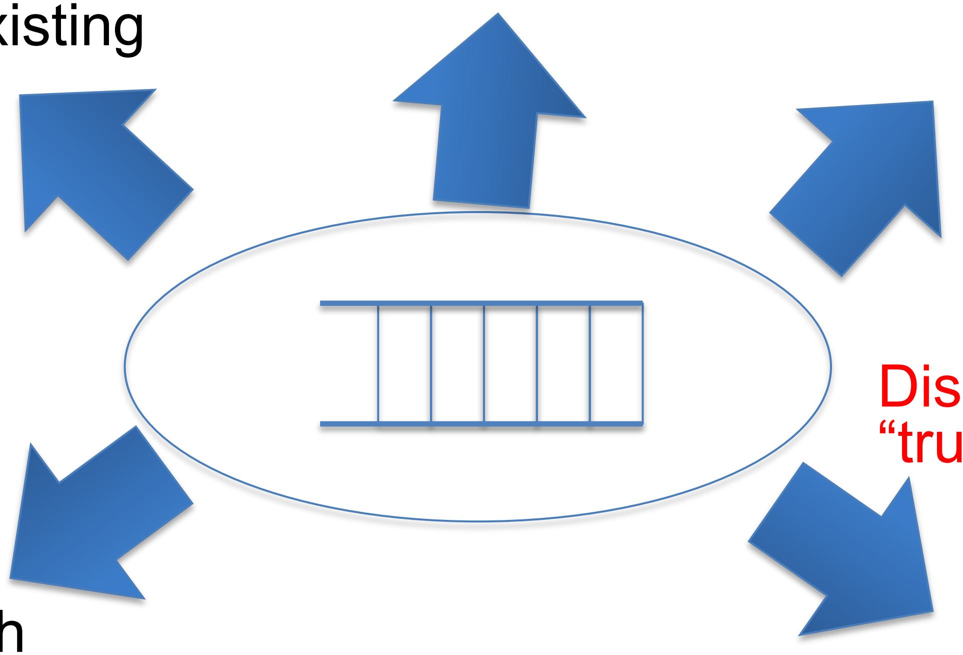
- Medics given access to all records they request
- Provided request is entered in a tamperproof log
- After emergency is over, logs are reviewed

Tamperproof log, but how?



- In an ad hoc network – limited access to public cloud
- Not all nodes can be trusted

Requirements of a tamperproof log



Availability

- Must be readable at all times
- Appendable “under normal circumstances”

Integrity

- Append-only
- No modification or deletion of existing records

Scrutinizable

- Protocol and implementation must be easy to understand
- Ideally formally verified

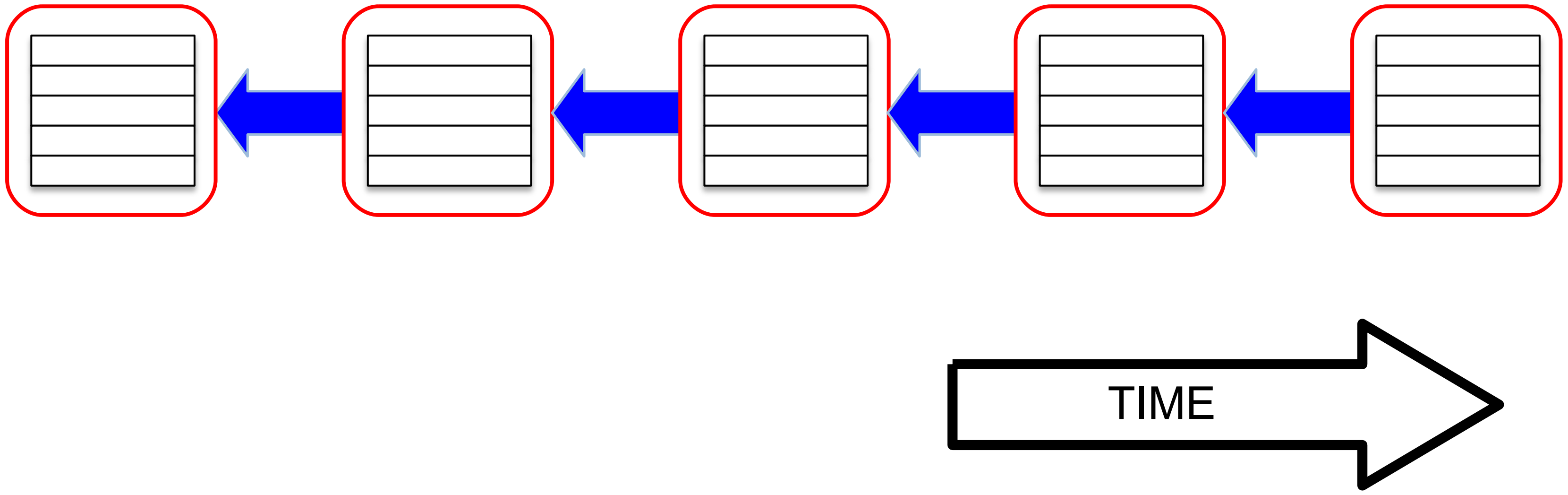
Performance

- Scale, high throughput, low latency, efficiency

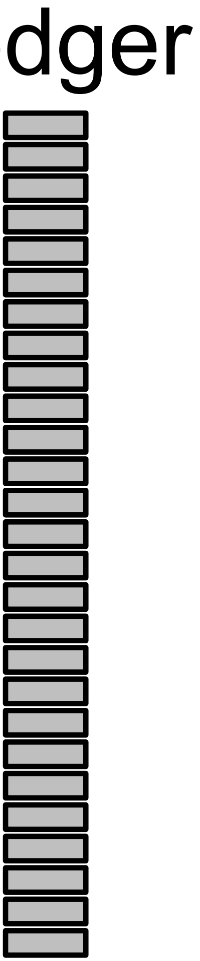
Distributed Trust, or “trustless”

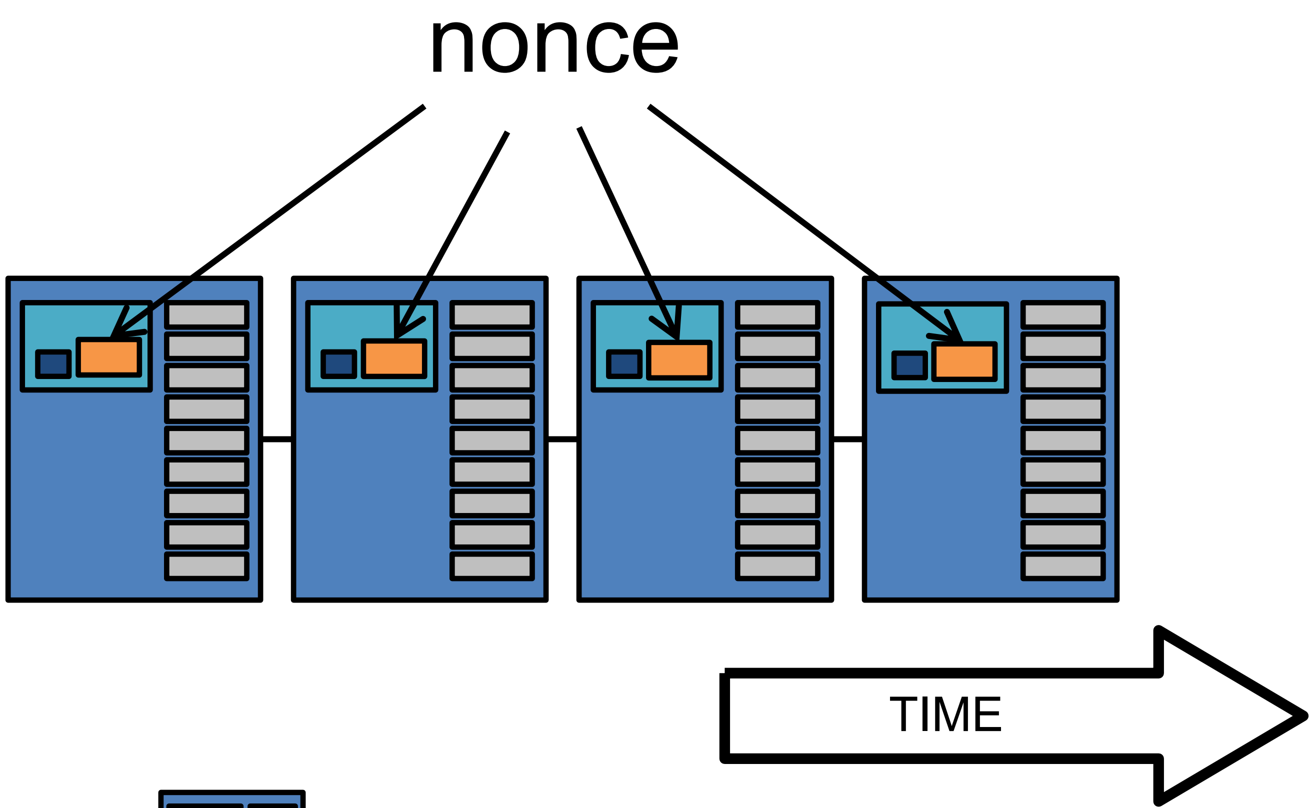
- Not under a single administrative domain
- Yet should be impersonation-resistant

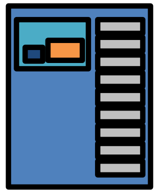
Blockchain as tamperproof log



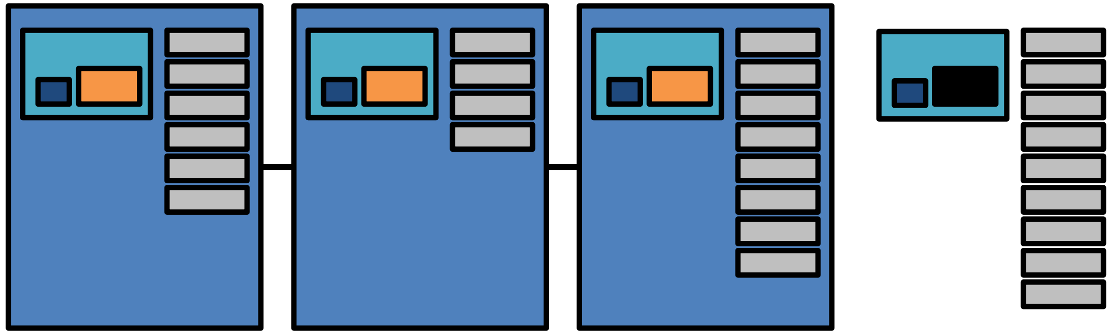
The Bitcoin Blockchain



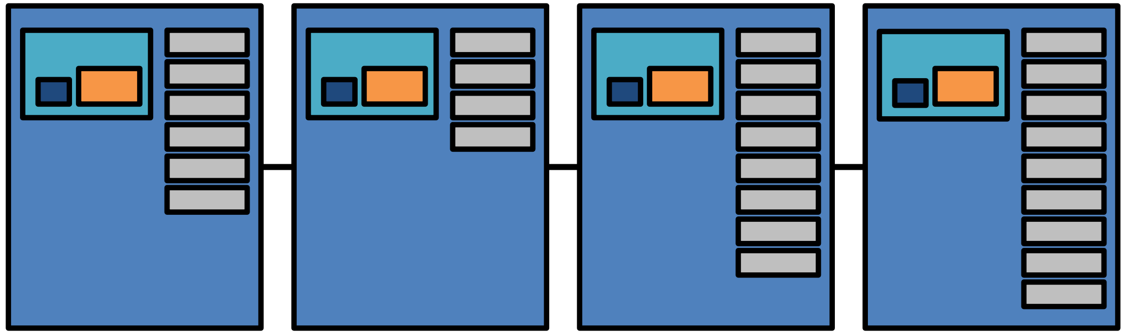


HASH() < ***target*** *“cryptopuzzle”*

The Bitcoin Blockchain



The Bitcoin Blockchain

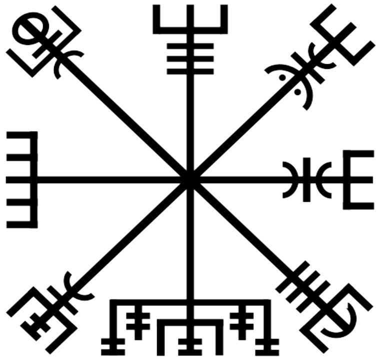


Bitcoin-style blockchains not an option

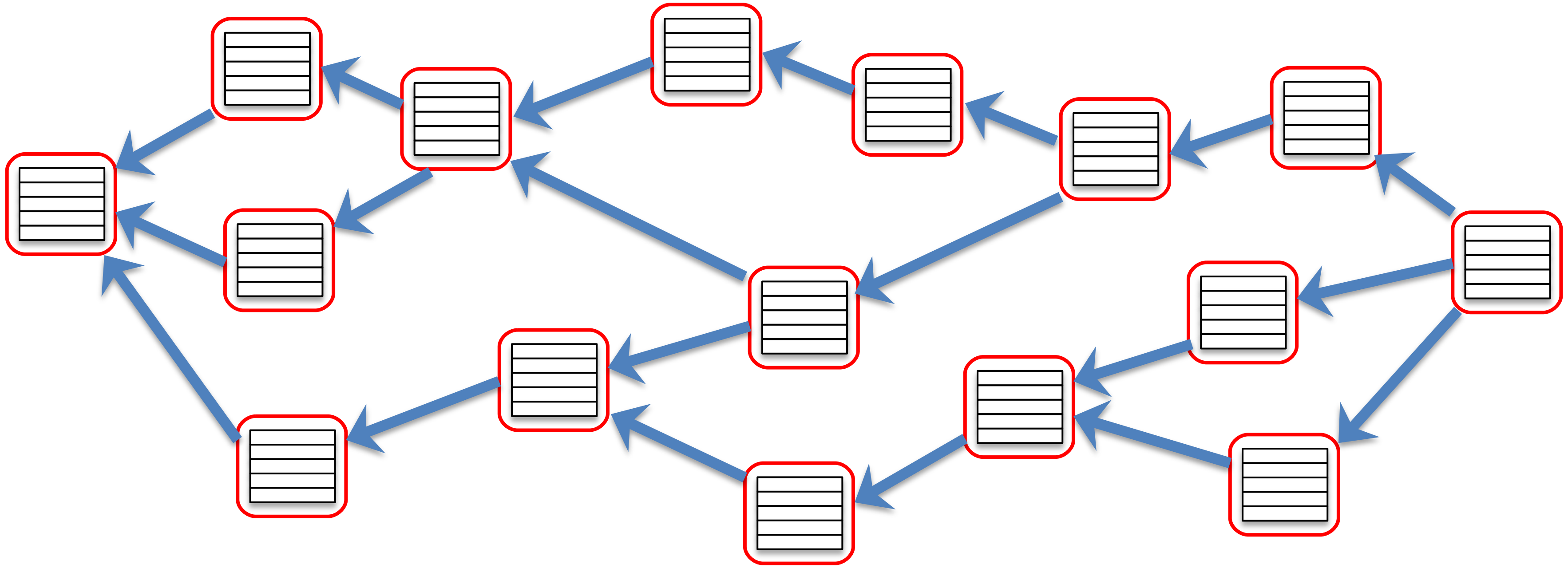
- Are computationally expensive – and thus battery-draining
- Require high network connectivity
  - Miners typically want to broadcast new blocks asap
    - first miner wins the prize
  - Protocol can recover from temporary network partitions, but leads to blocks being discarded and work wasted, as well as security issues
- Lack of decentralization harms security

“Permissioned” blockchains can dispense with proof of work

- Blockchain doubles as a PKI
- Owner’s self-signed certificate in genesis block
- Additional users added/removed by placing certificates/revocations on blockchain
- But system-wide consensus is not an option either



Vegvisir: tolerate branches

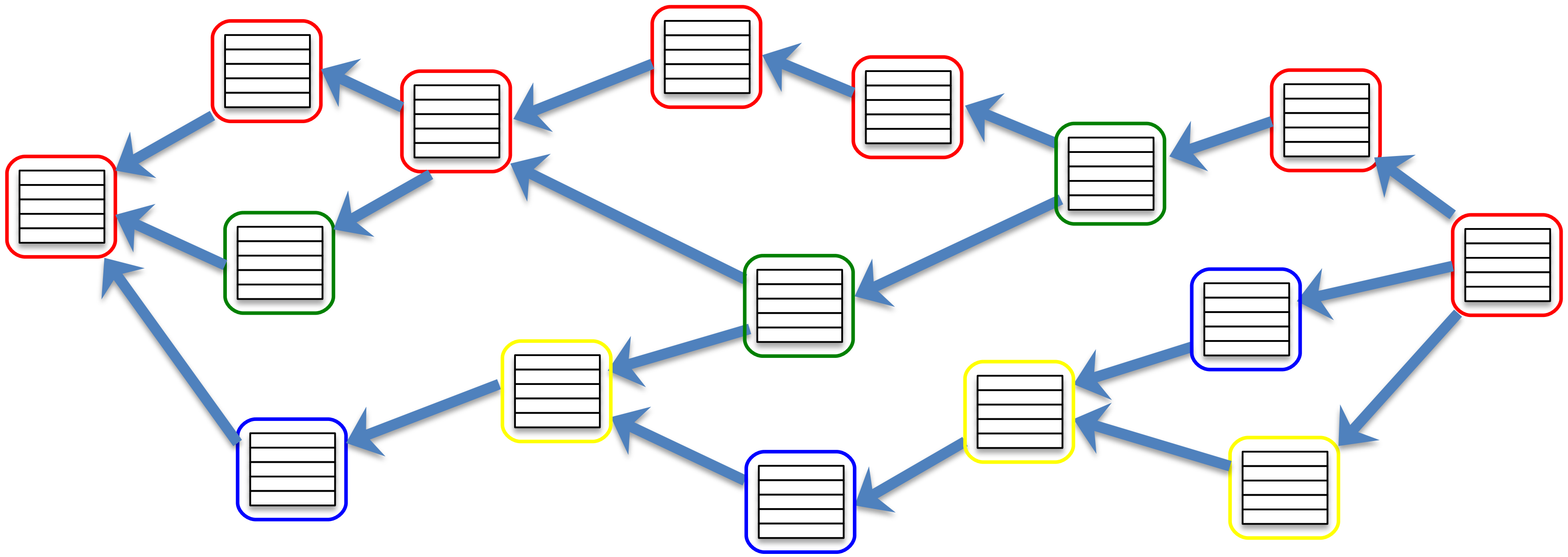


- Leads to DAG structure instead of linear blockchain
- Not good for cryptocurrencies…
- Still maintains full causal history of events

Properties

- Availability:
  - blocks, once added, cannot be removed
- Integrity:
  - unique genesis block (sink)
  - each DAG has a unique “leader block” (source)
  - each DAG is connected (and loop-free…)
  - each block signed by authorized principal
  - blocks signed by same (honest) principal on unique path
- Confidentiality
  - end-to-end encryption of transactions (optional)

Integrity



- Maximum “width” is determined by the number of principals

  (Byzantine principals can temporarily create higher width)

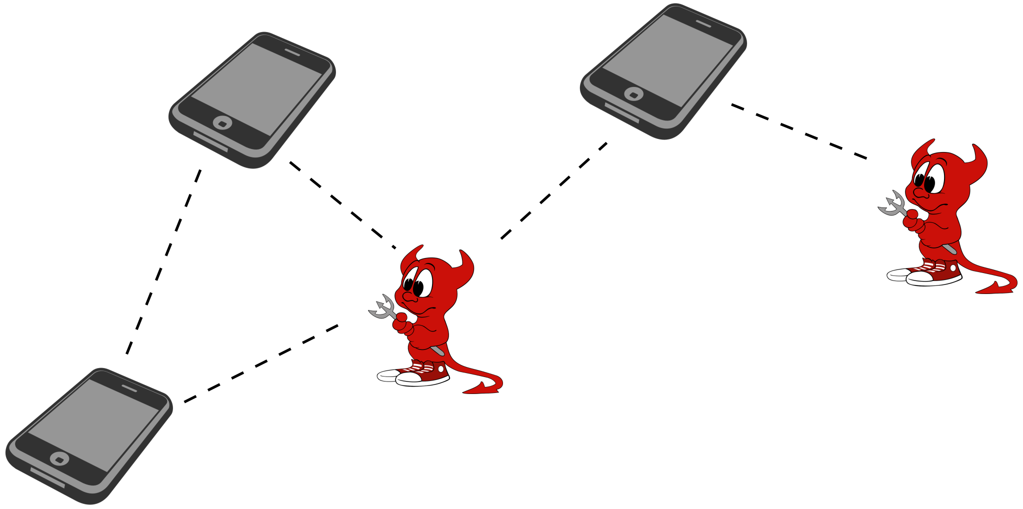
- Signed blocks on different paths are “proof-of-misbehavior”

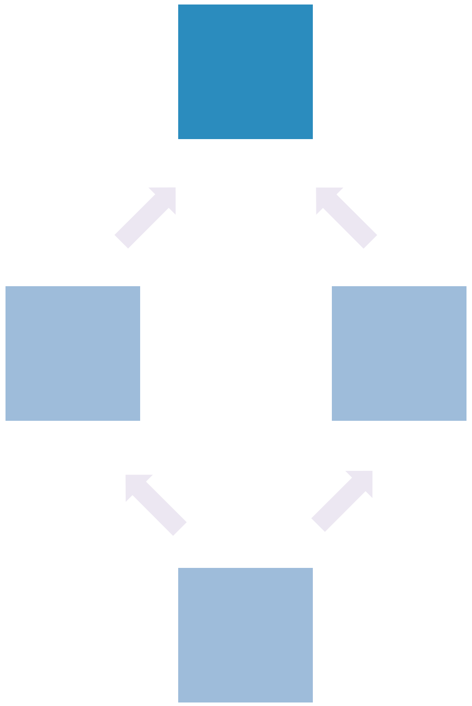
Availability: Proof-of-Witness

🟦 Valid block

▨ Not yet valid block

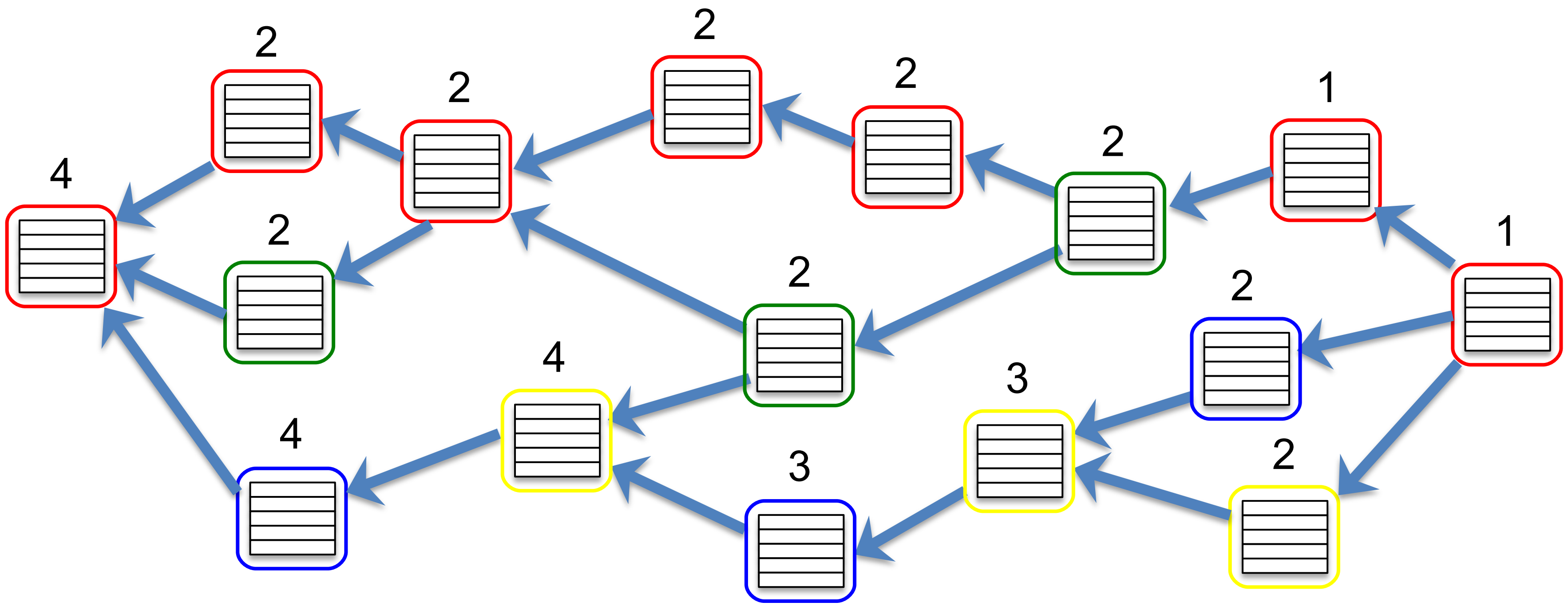
No more than *k* malicious nodes in any neighborhood



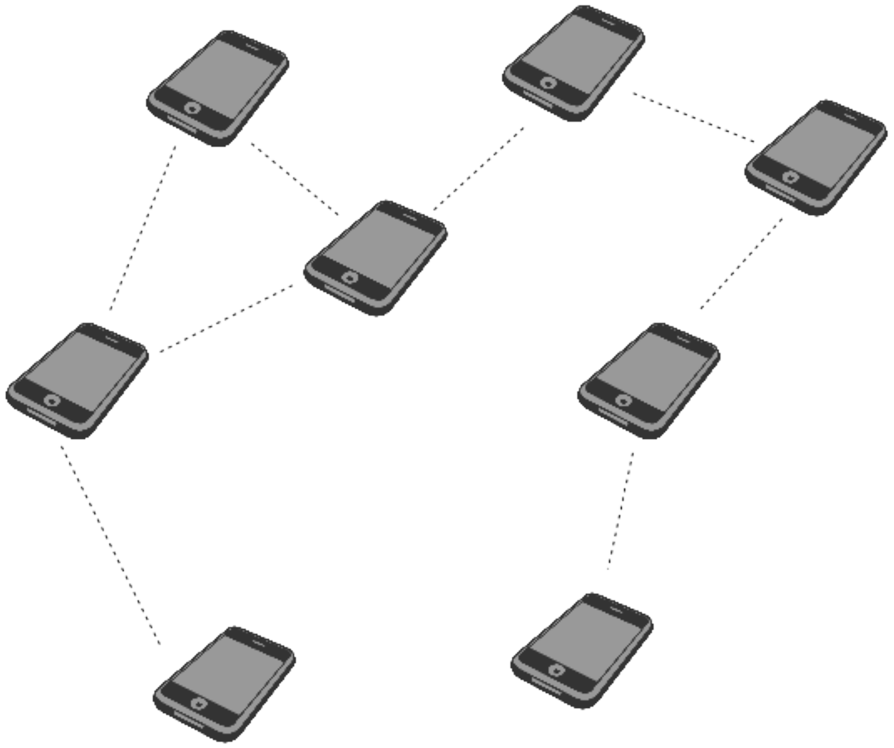


- Block will survive if >k witnesses
- If one block has PoW, so has all its ancestor blocks
- Research question: who makes good witnesses?

Counting Witnesses

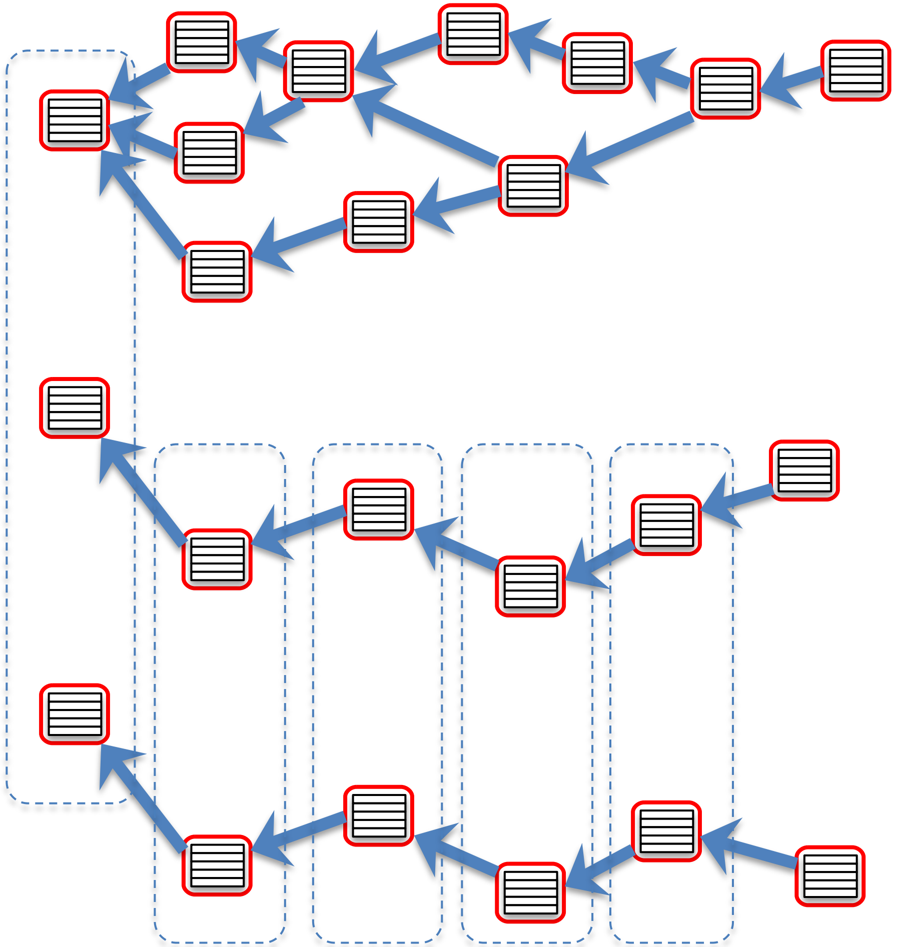


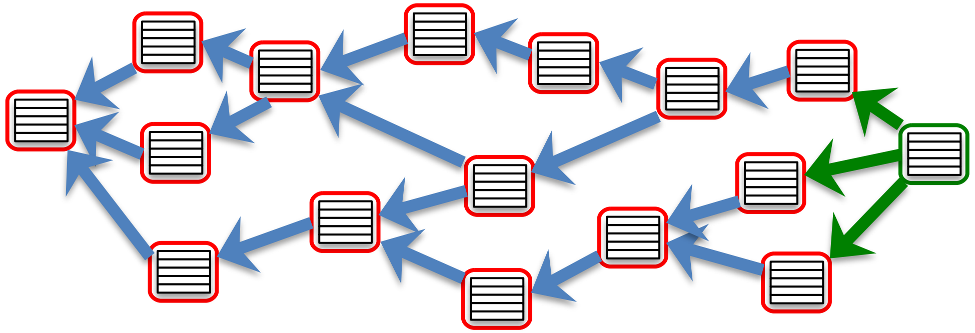
Blocks gossiped over ad hoc network



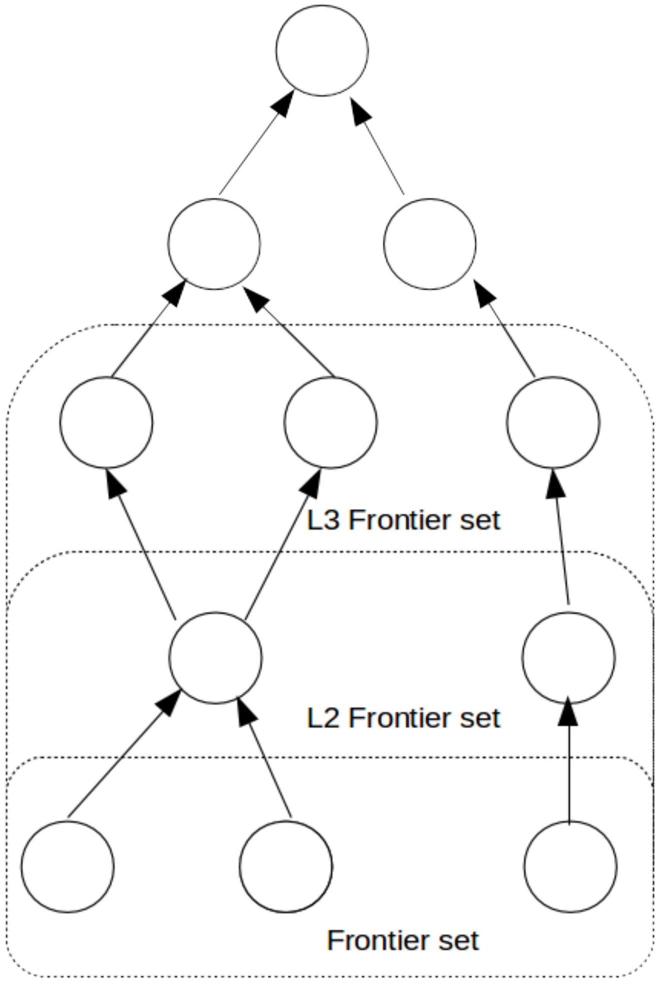
Heterogeneous, opportunistic networking

Reconciliation



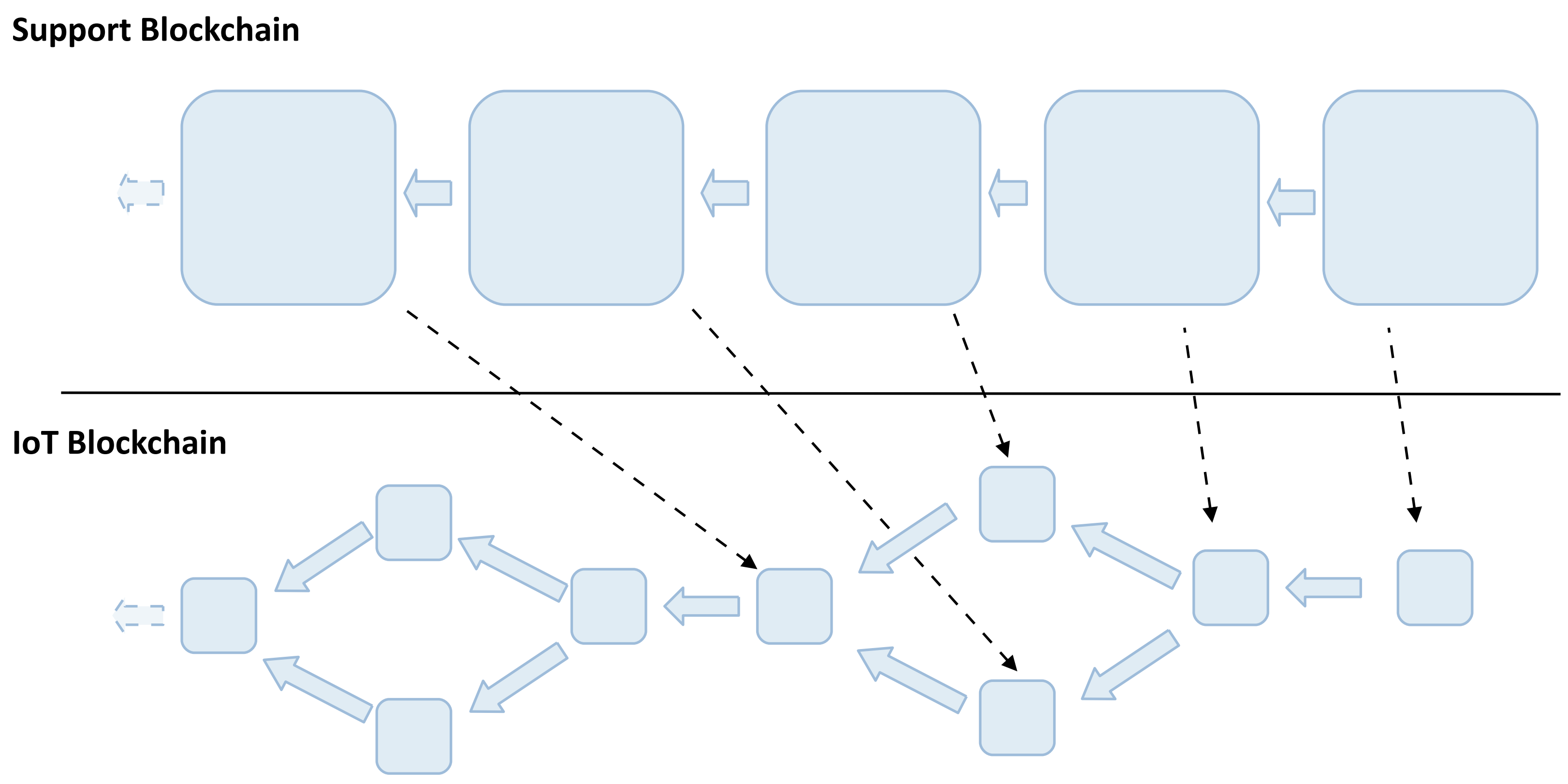


DAG Reconciliation



Peers exchange frontier sets incrementally

Offloading to "support blockchain"



- Allows regular peers to discard old blocks when storage space is low
- Design invariant: availability of a block is monotonically increasing

Interpreting Vegvisir

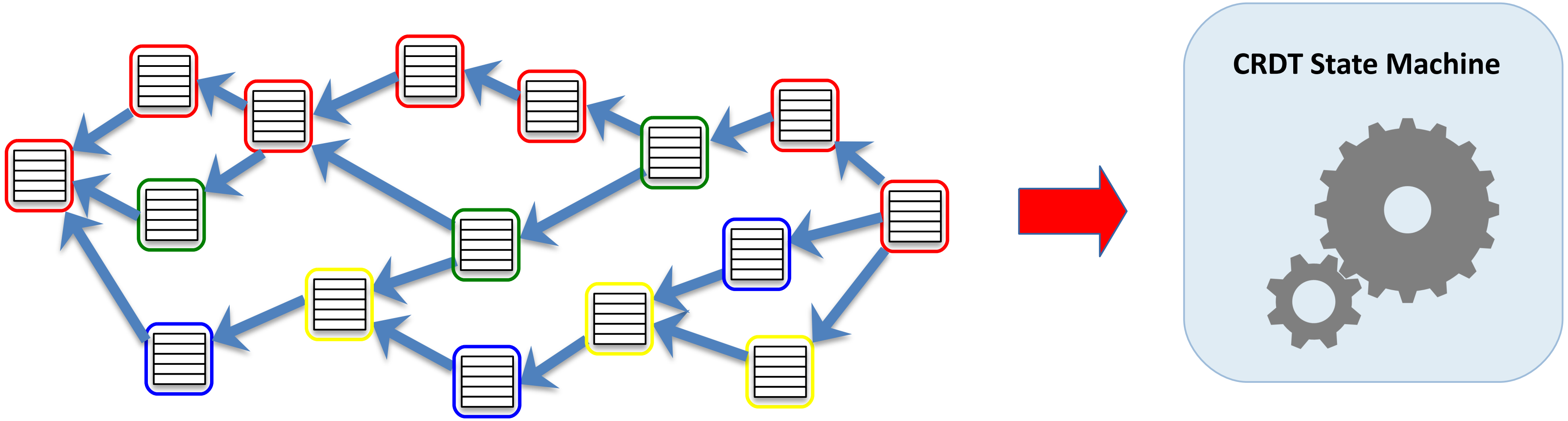
- Vegvisir provides a shared, tamperproof data repository that keeps track of data provenance and distributes trust over peers
- Only requirement is that updates on shared data structure in some sense commute

Conflict-Free Replicated Datatypes (CRDTs)

- Updates must be associative, commutative, idempotent
- Nodes can be updated independently
- Basic CRDTs form registers, counters, sets
- Can be combined and composed

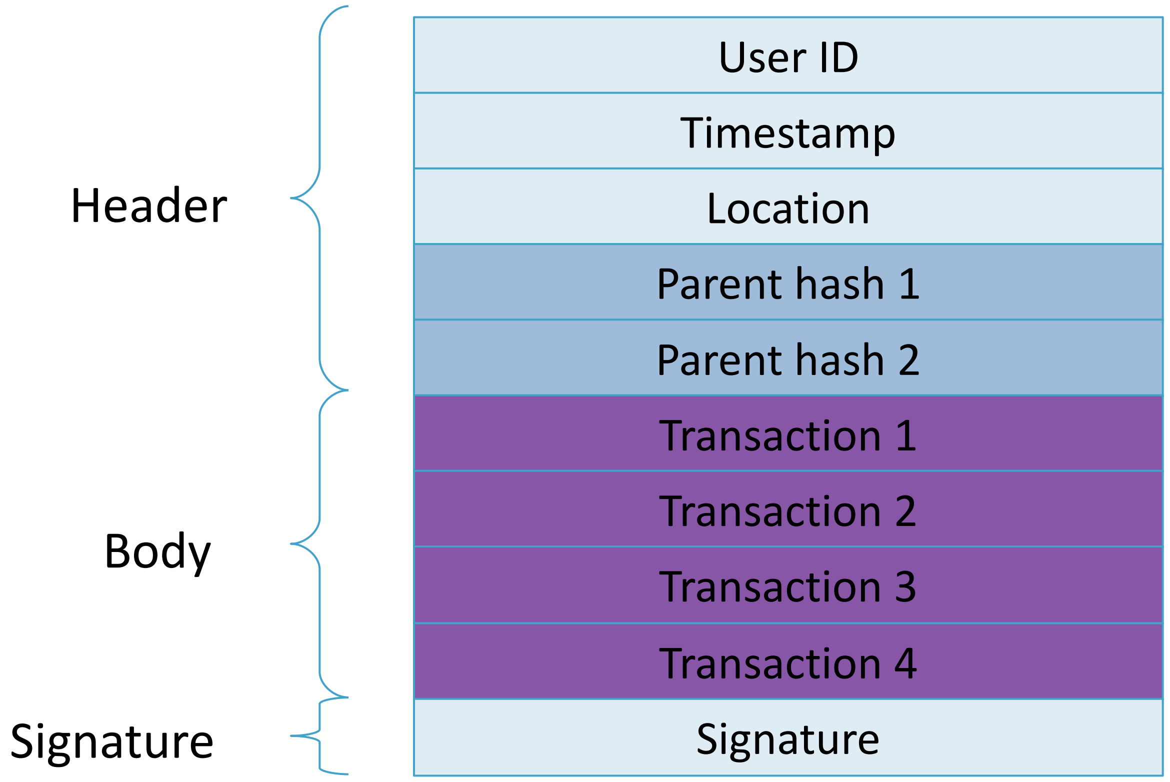
Vegvisir has two main components

- Blockchain itself
- CRDT state machine



Operations only applied if PoW available

Vegvisir Block Structure



Header

User ID

Timestamp

Location

Parent hash 1

Parent hash 2

Body

Transaction 1

Transaction 2

Transaction 3

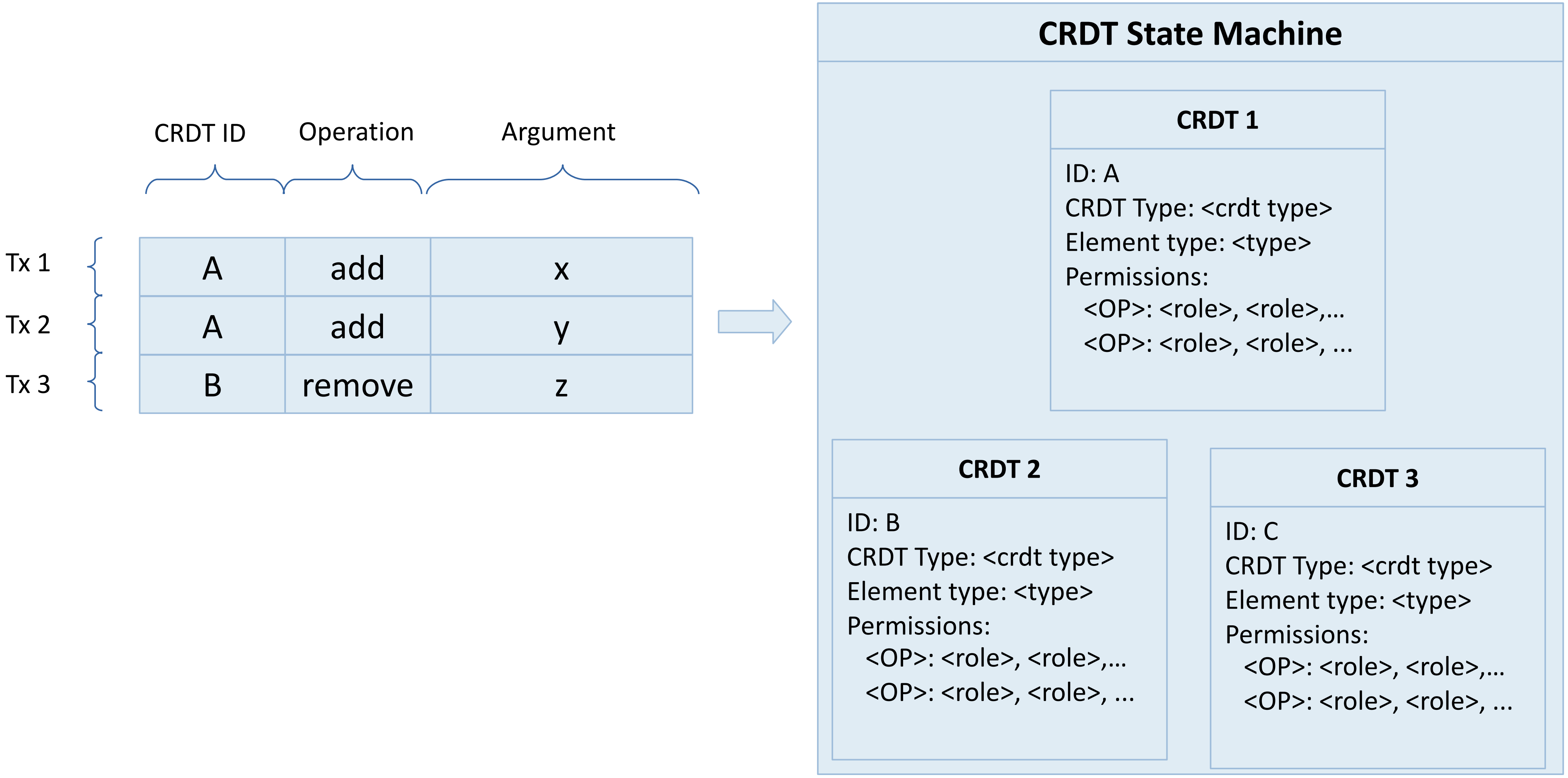
Transaction 4

Signature

Signature

Blocks are certificates

Transactions manipulate CRDTs



	CRDT ID	Operation	Argument
Tx 1	A	add	x
Tx 2	A	add	y
Tx 3	B	remove	z

CRDT State Machine

CRDT 1

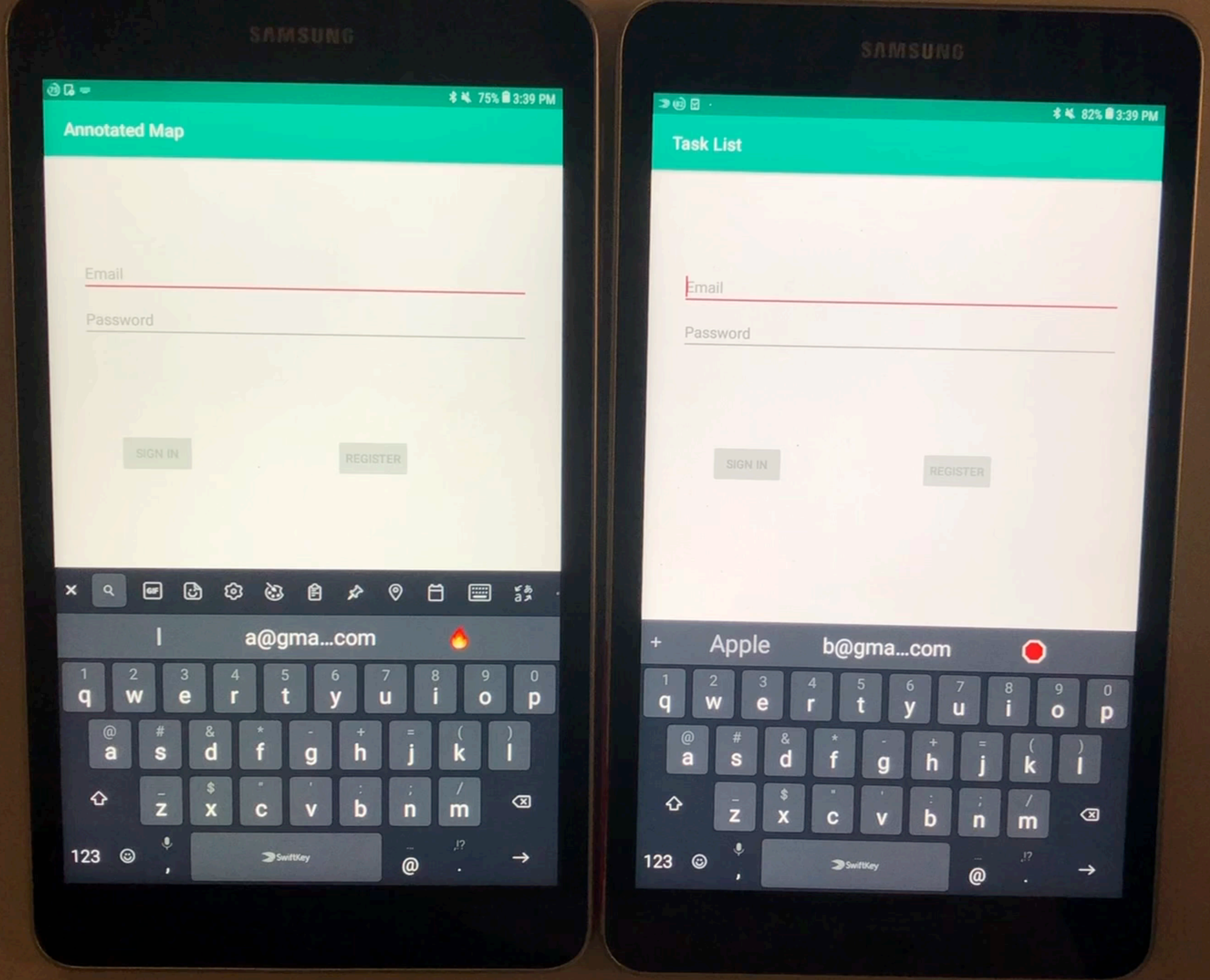
ID: A
CRDT Type: <crdt type>
Element type: <type>
Permissions:
  <OP>: <role>, <role>,…
  <OP>: <role>, <role>, ...

CRDT 2

ID: B
CRDT Type: <crdt type>
Element type: <type>
Permissions:
  <OP>: <role>, <role>,…
  <OP>: <role>, <role>, ...

CRDT 3

ID: C
CRDT Type: <crdt type>
Element type: <type>
Permissions:
  <OP>: <role>, <role>,…
  <OP>: <role>, <role>, ...


SAMSUNG
75% 3:39 PM
Annotated Map
Email
Password
SIGN IN
REGISTER
a@gma...com
SAMSUNG
82% 3:39 PM
Task List
Email
Password
SIGN IN
REGISTER
Apple
b@gma...com

Membership

- One special CRDT (2P) maintains membership
    - add-membership
    - revoke-membership
- Proof-of-misbehavior also implicitly revokes membership
- Only members can add new blocks

ARM TrustZone

- ARM TrustZone “secure worlds” can help:
  - Who is a good witness?
    - secure access to device location and time
  - Check PoW and provide access to secured data
  - Secure sensor values
    - secure retrieval of sensor values

Conclusion

- Vegvisir is a DAG-based blockchain to allow for partitioned operations
  - *not for higher throughput per se*
- Replaces Proof-of-Work with *“Proof-of-Witness”*
- CRDTs enable consistently evolving views
- Prototype available for Android devices

#PSCR2019

Come back for the

Next Session