Cryptographic Foundations
of
Blockchains

Hong-Sheng Zhou
Virginia Commonwealth University
http://www.people.vcu.edu/~hszhou/
hongsheng.zhou@gmail.com

Plan

- Bitcoin basics
- Cryptographic foundations
- Nakamoto’s protocol
- Alternative mechanisms
- Crypto on the blockchain

blockchain in the news

索 引 号：	000014349/2017-00162	主题分类：	工业、交通\信息产业（含电信）
发文机关：	国务院	成文日期：	2017年08月13日
标　　题：	国务院关于进一步扩大和升级信息消费持续释放内需潜力的指导意见		
发文字号：	国发〔2017〕40号	发布日期：	2017年08月24日
主 题 词：			

国务院关于进一步扩大和升级信息消费持续释放内需潜力的指导意见

国发〔2017〕40号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

近年来，随着互联网技术与经济社会深度融合，我国信息消费快速发展，正从以线上为

相关报道

国务院印发《关于进一步扩大和升级信息消费持续释放内需潜力的指导意见》

图解

（七）提升信息技术服务能力。支持大型企业建立基于互联网的“双创”平台，为全社会提供专业化信息服务。发挥好中小企业公共服务平台作用，引导小微企业创业创新示范基地平台化、生态化发展。鼓励信息技术服务企业积极发展位置服务、社交网络等新型支撑服务及智能应用。支持地方联合云计算、大数据骨干企业为当地信息技术服务企业提供咨询、研发、培训等技术支持，推动提升“互联网+”环境下的综合集成服务能力。鼓励利用开源代码开发个性化软件，开展基于区块链、人工智能等新技术的试点应用。

Bitcoin Blockchain

How Bitcoin works under the hood

many slides of this part are from Professor Roger Wattenhofer

The Bank of Bitcoin

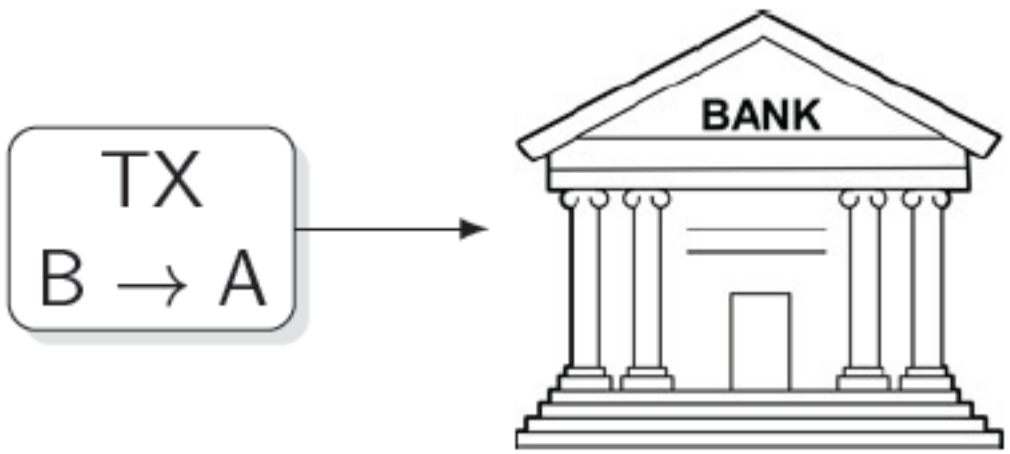
The Bank of Bitcoin

User	Balance
A	2
B	5
C	8

ledger

a ledger for all user activities

The Bank of Bitcoin



User	Balance
A	2
B	5
C	8

ledger

a ledger for all user activities

The Bank of Bitcoin

TX
B → A

User	Balance
A	~~2~~ 4
B	~~5~~ 3
C	8

ledger

a ledger for all user activities

Opening an Account in Bitcoin

User

cryptographic tool:
digital signature scheme

private key for signature generation

public key for signature verification

public key = user account address

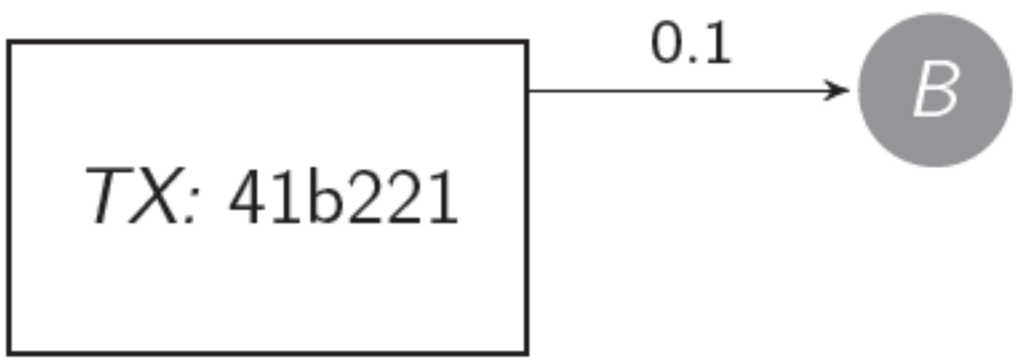
Transferring Bitcoins

User

TX: 41b221

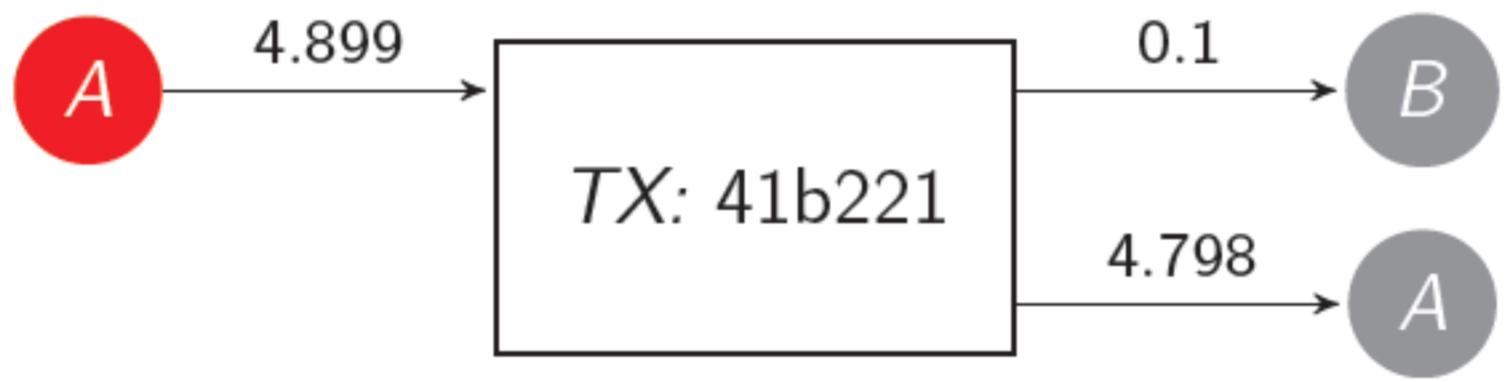
user A transfers 0.01 coins to user B

Transferring Bitcoins



user A transfers 0.01 coins to user B

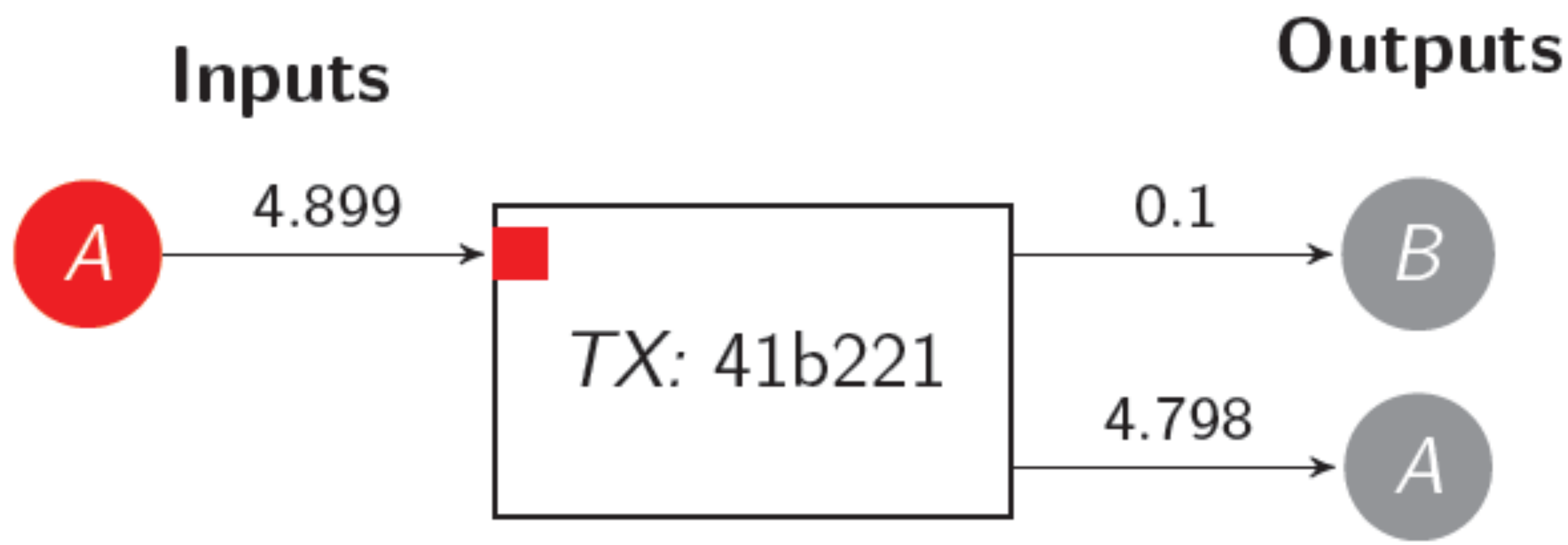
Transferring Bitcoins



user A transfers 0.01 coins to user B

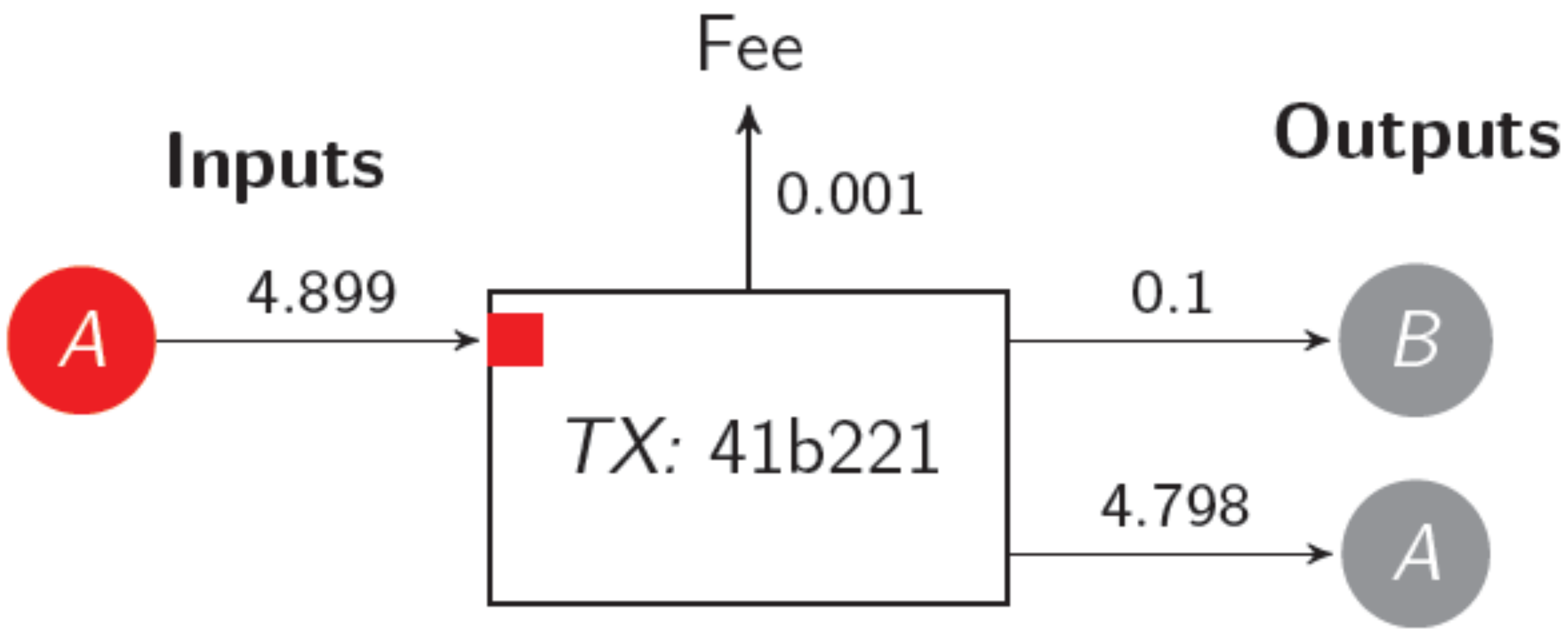
Transferring Bitcoins

User



user A transfers 0.01 coins to user B

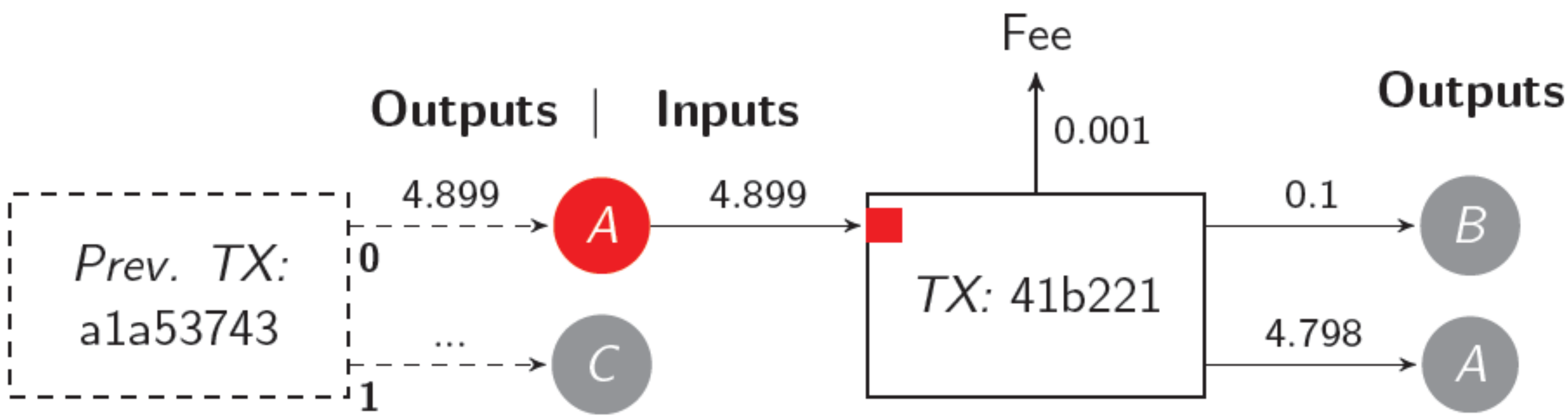
Transferring Bitcoins



user A transfers 0.01 coins to user B

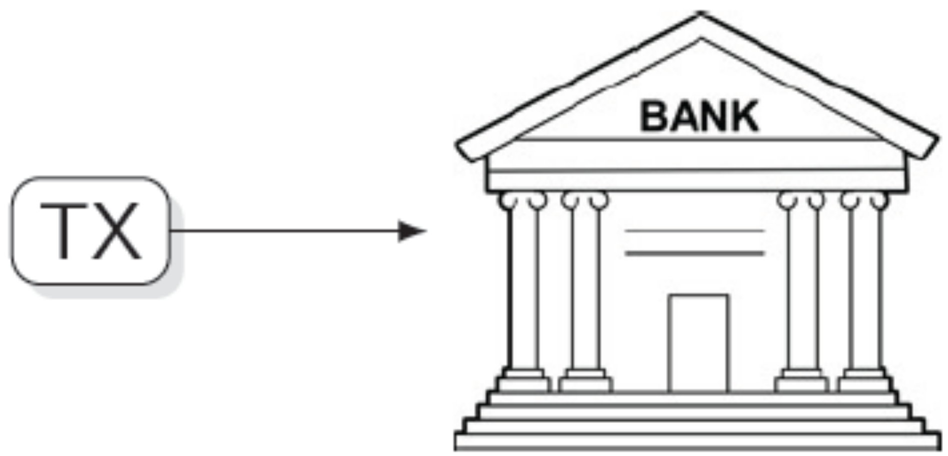
Transferring Bitcoins

User



user A transfers 0.01 coins to user B

Distributing the Bank



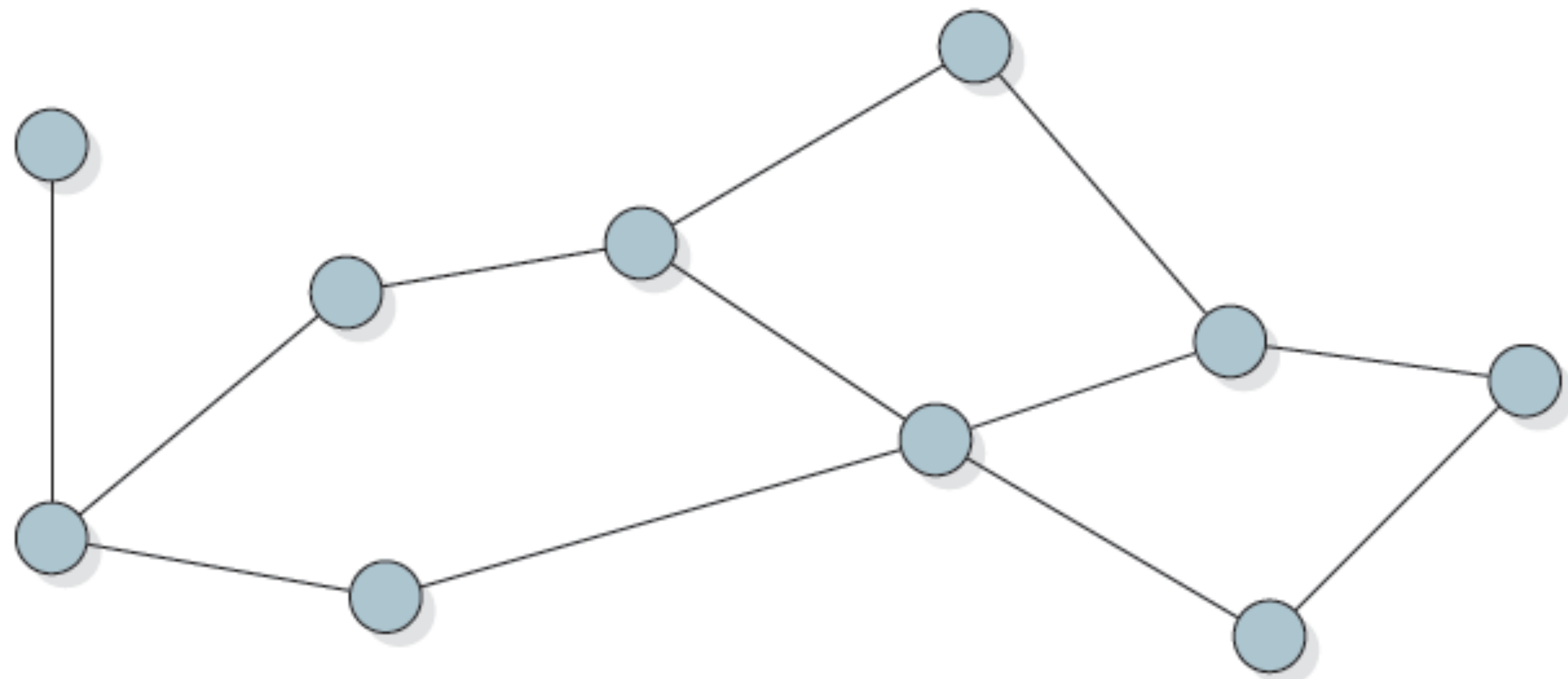
User	Balance
A	2
B	5
C	8

ledger

distribute the ledger

Distributing the Bank

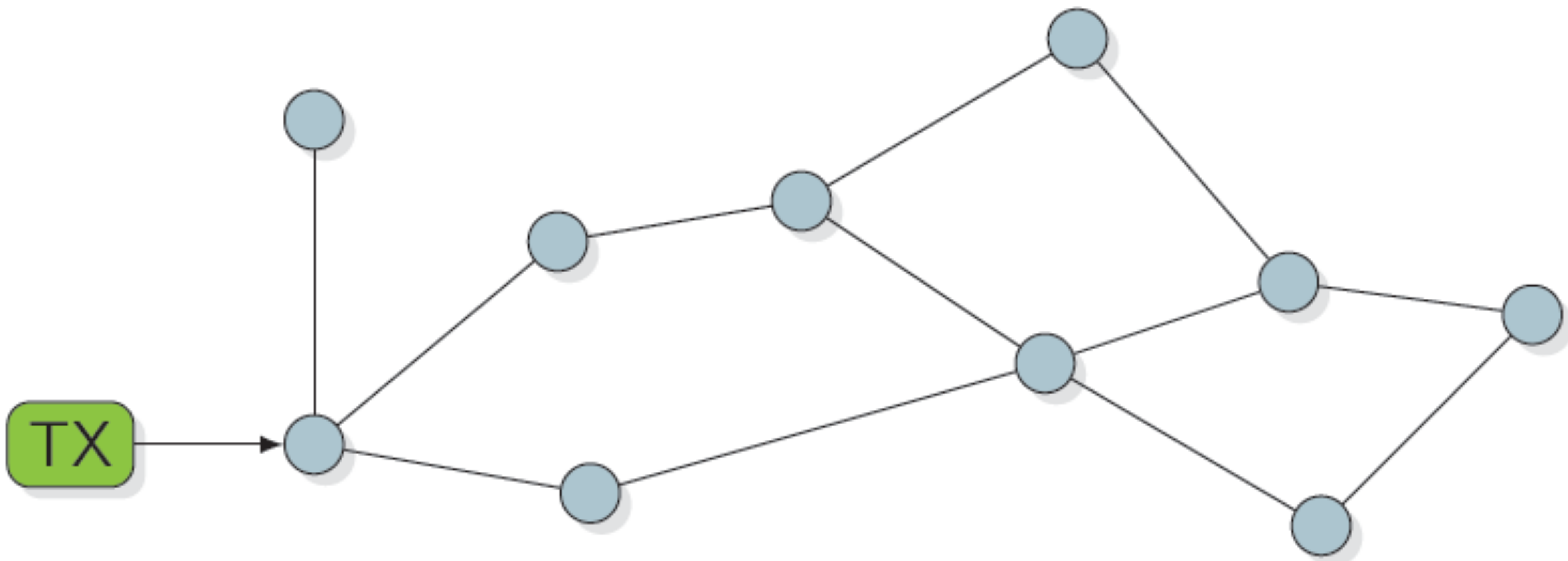
Miner



each node has its local ledger

Distributing the Bank

Miner

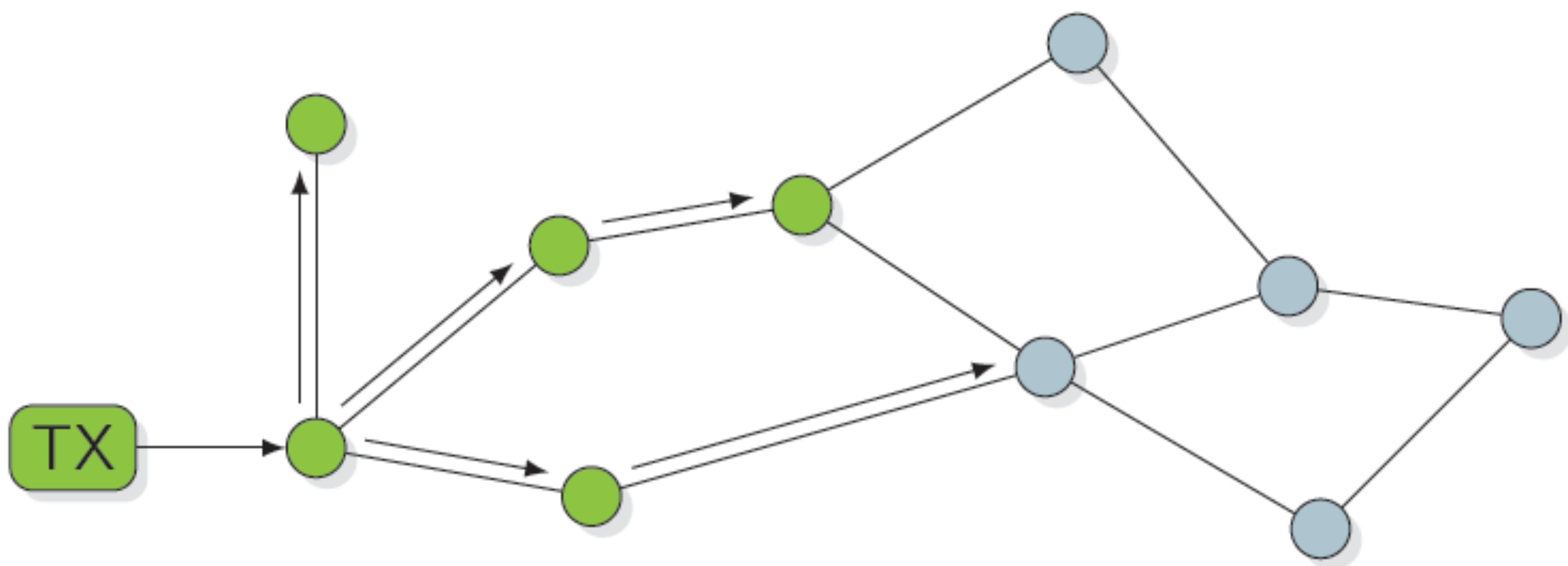


updates its local ledger once receives new transactions

each node has its local ledger

Distributing the Bank

Miner

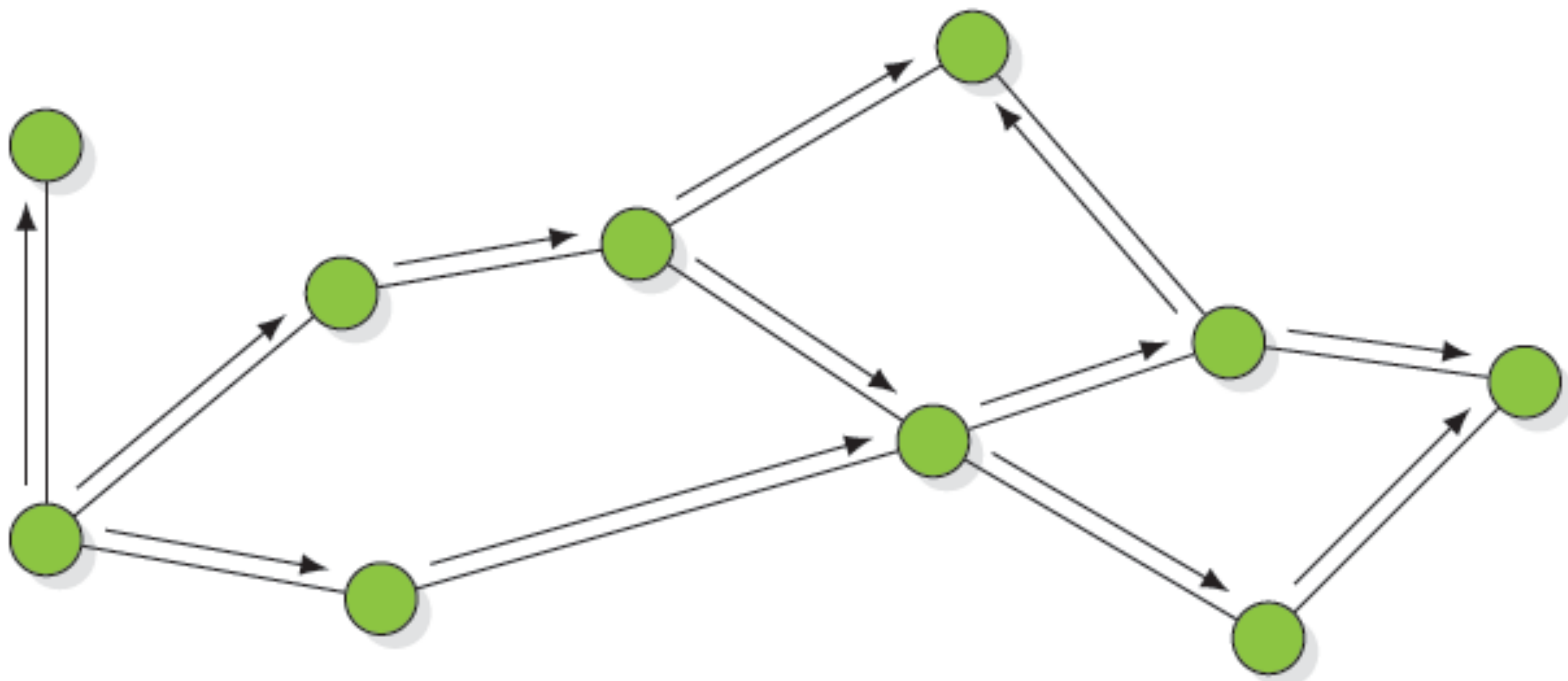


updates its local ledger once receives new transactions

each node has its local ledger

Distributing the Bank

Miner

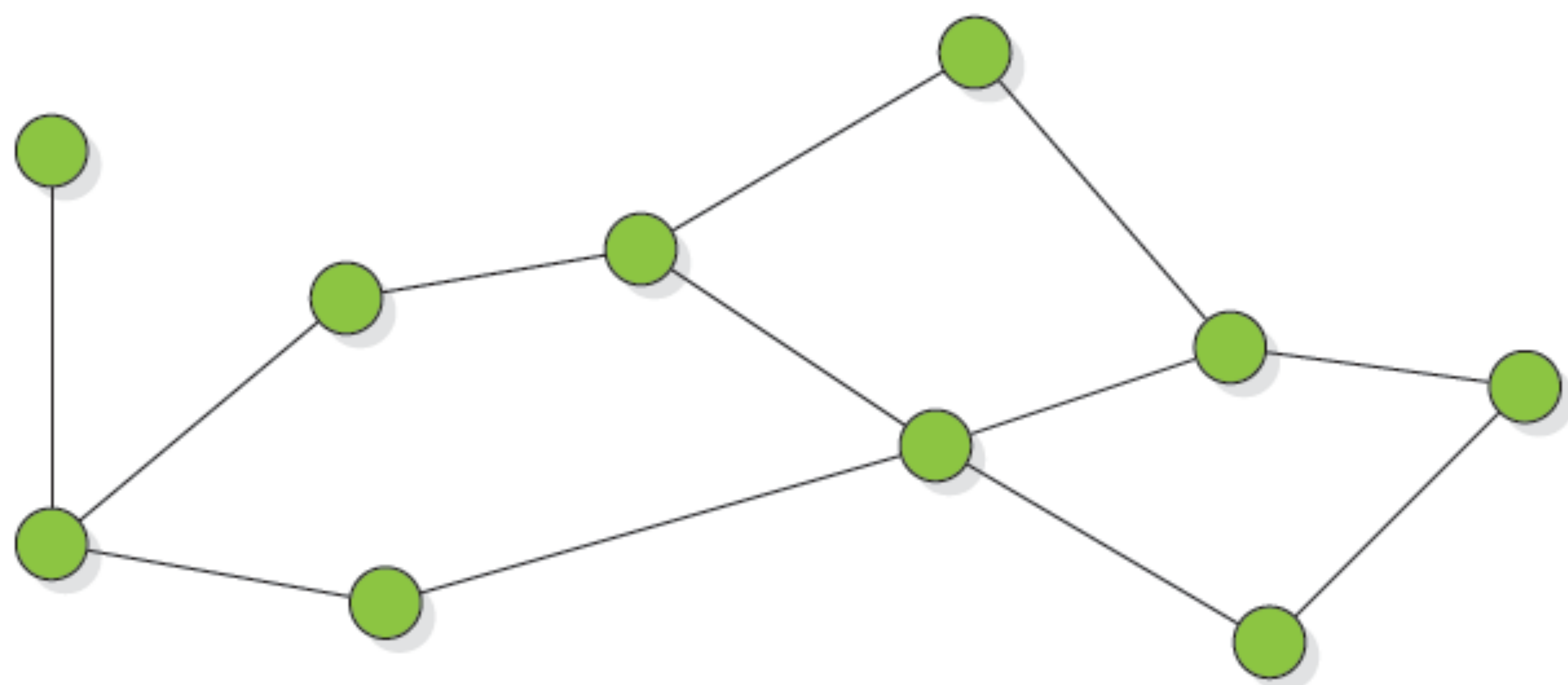


updates its local ledger once receives new transactions

each node has its local ledger

Distributing the Bank

Miner

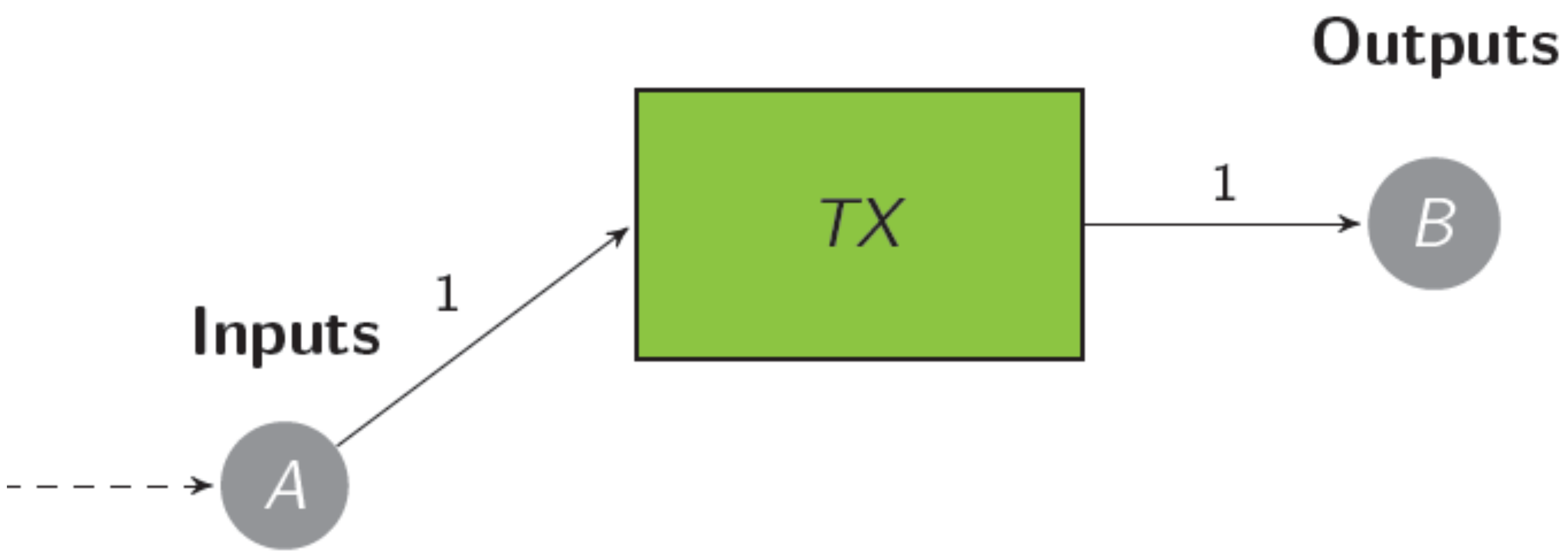


updates its local ledger once receives new transactions

each node has its local ledger

Doublespending

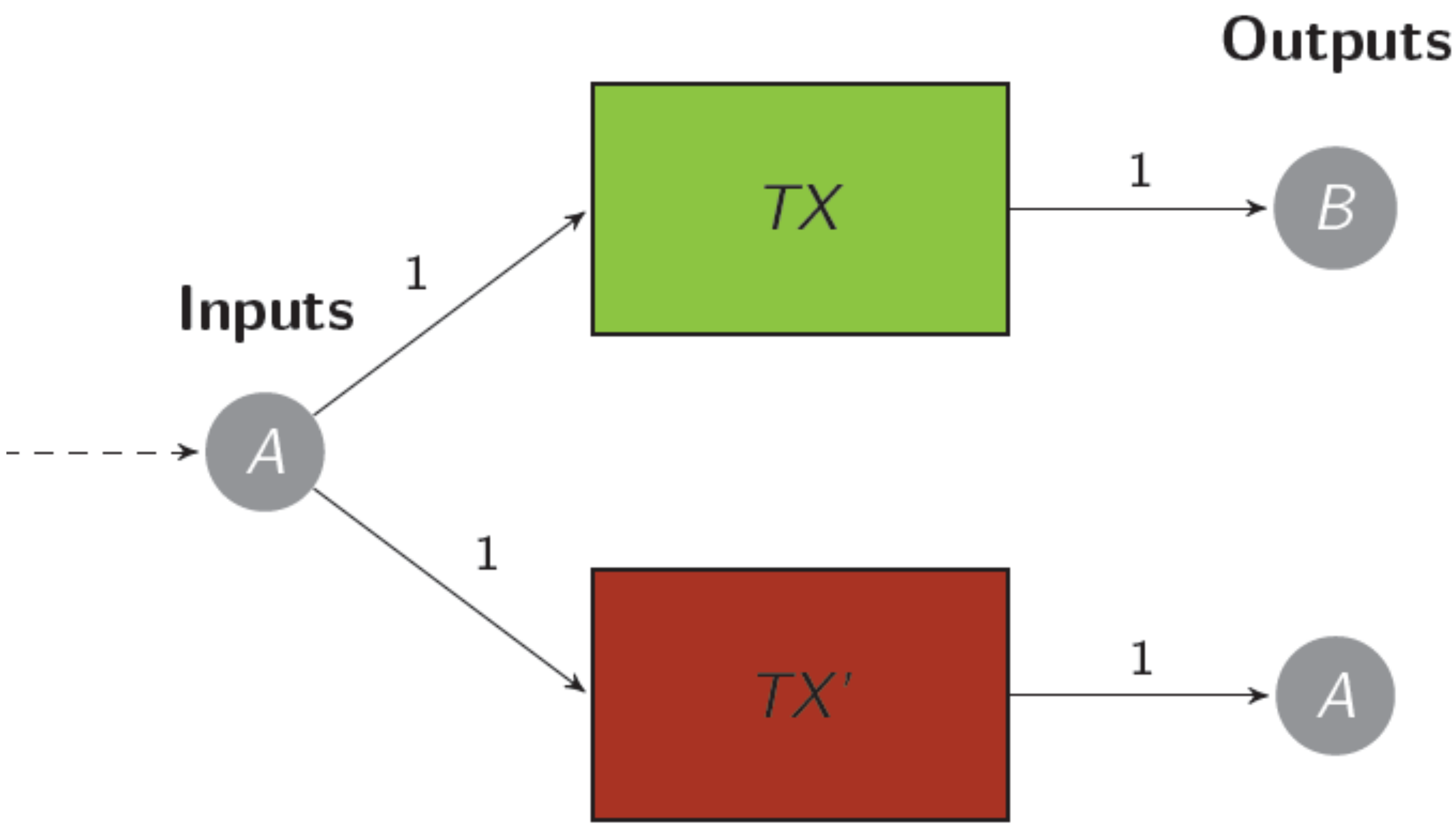
User



conflicted transactions could be generated

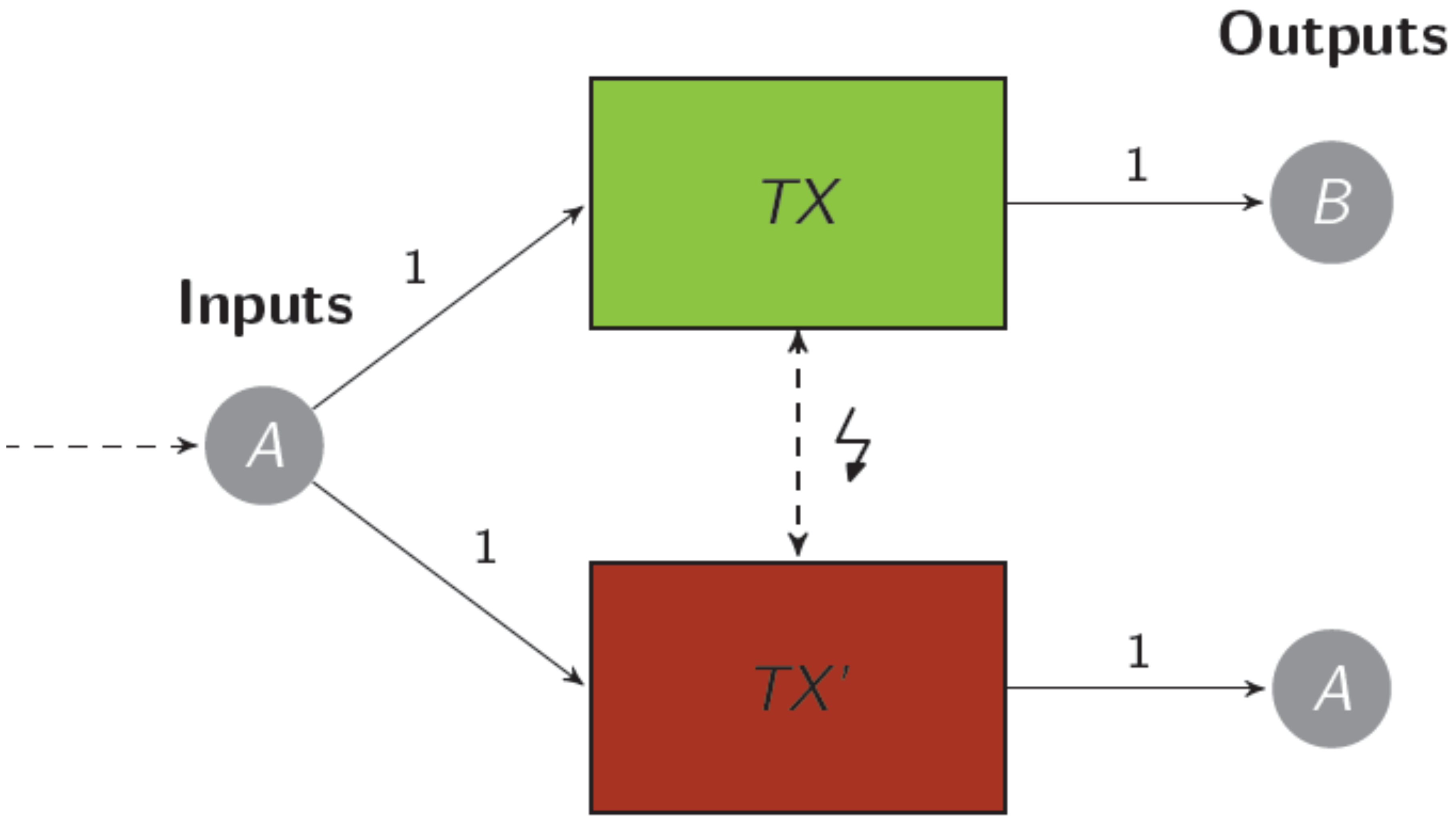
Doublespending

User



conflicted transactions could be generated

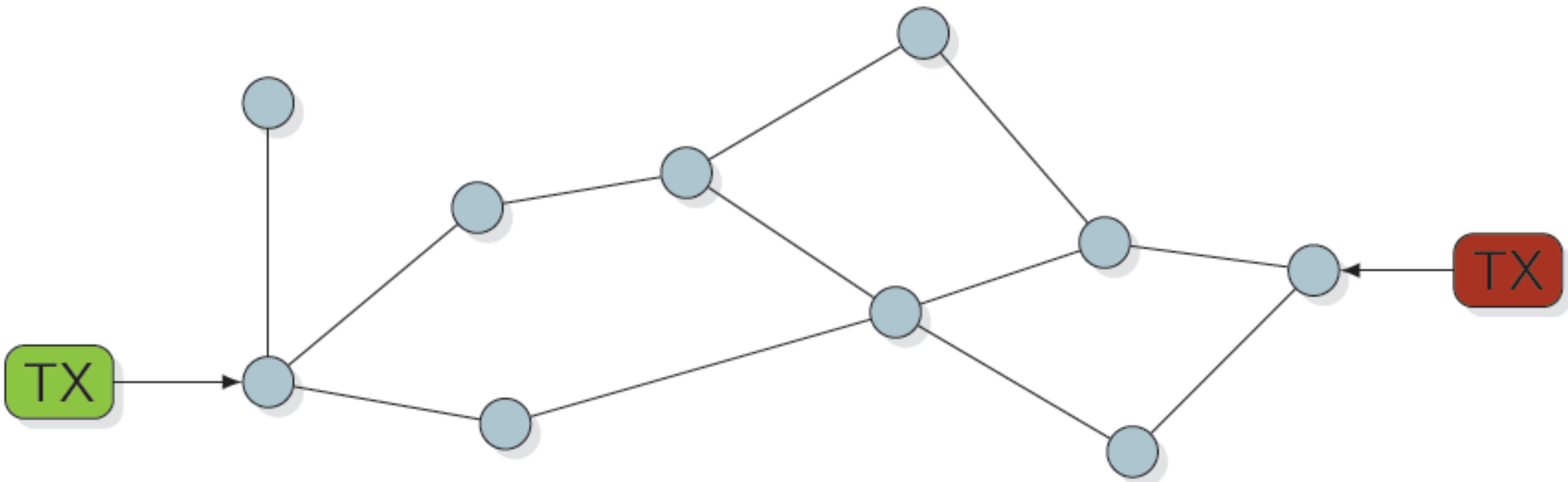
Doublespending



conflicted transactions could be generated

Transaction Conflicts

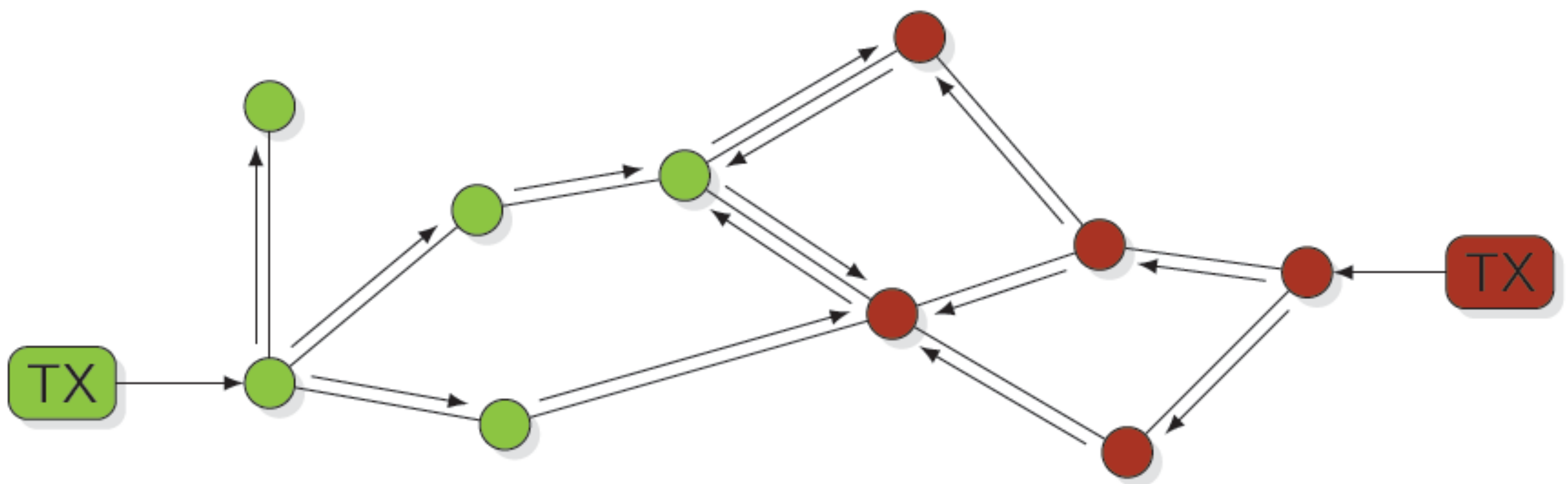
Miner



conflicted transactions appear in the network

Transaction Conflicts

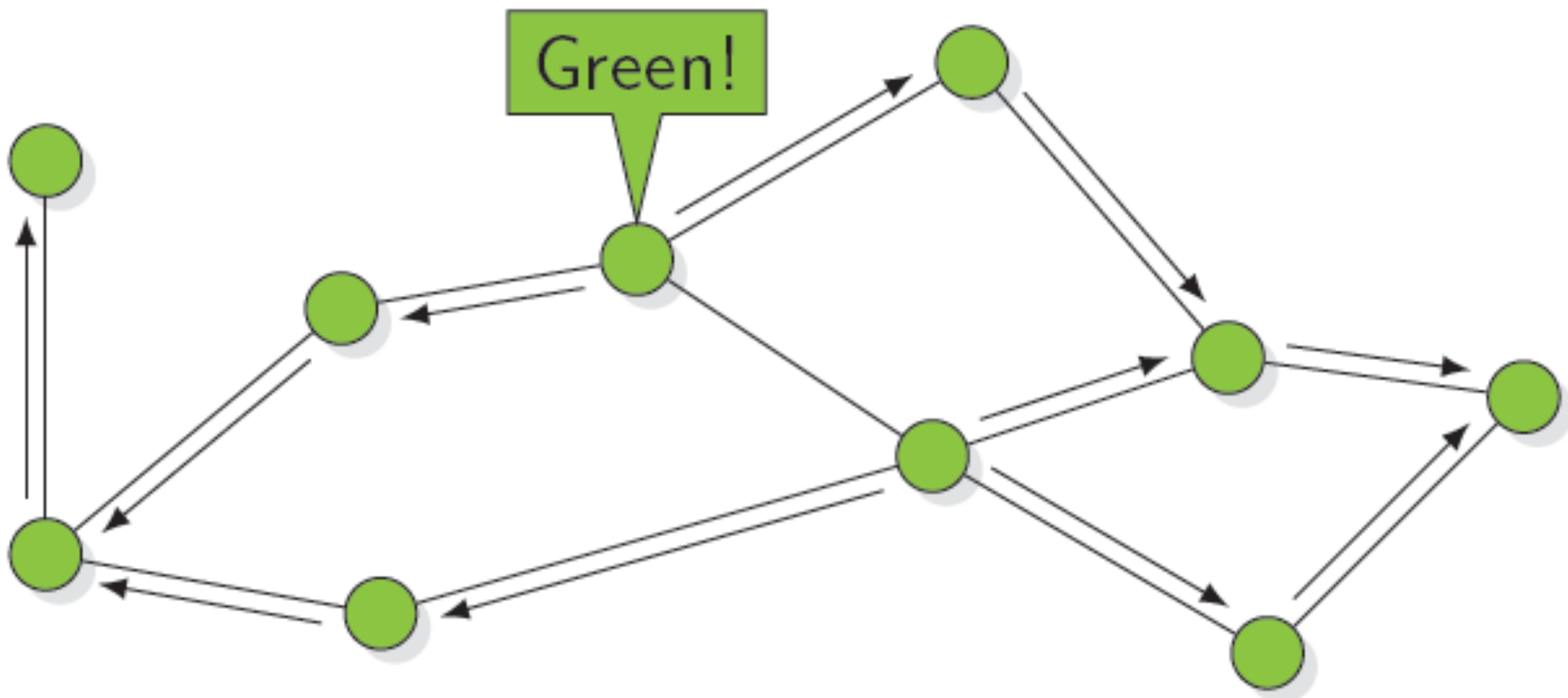
Miner



different nodes may have different local ledgers

conflicted transactions appear in the network

Resolving Conflicts



to resolve the conflicts, the same ledger must be agreed

How to Choose a Leader?

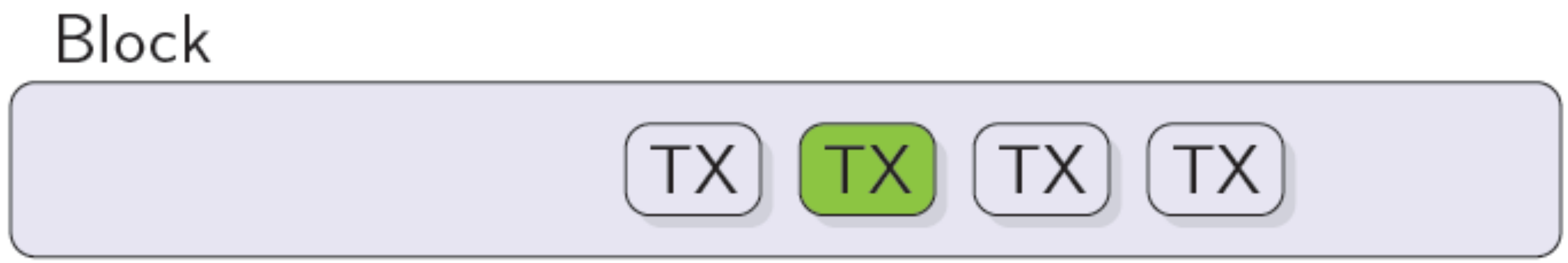
Proof-of-Work

Miner

cryptographic tool: hash function

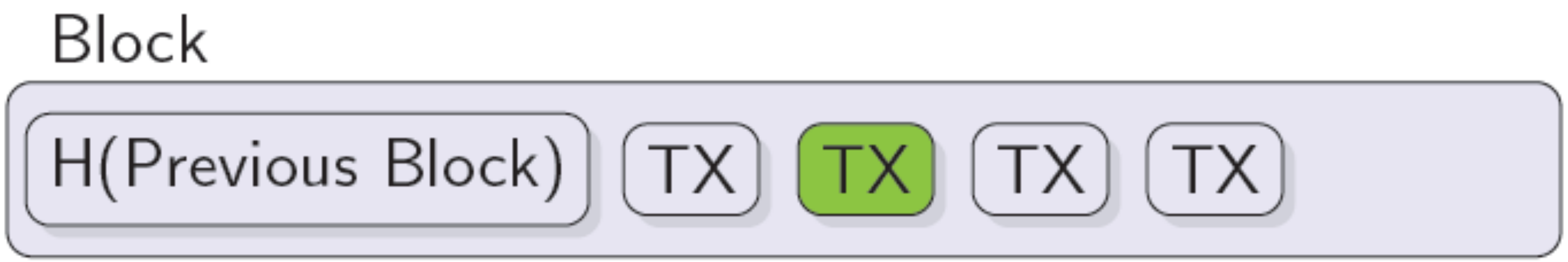
Proof-of-Work

Miner



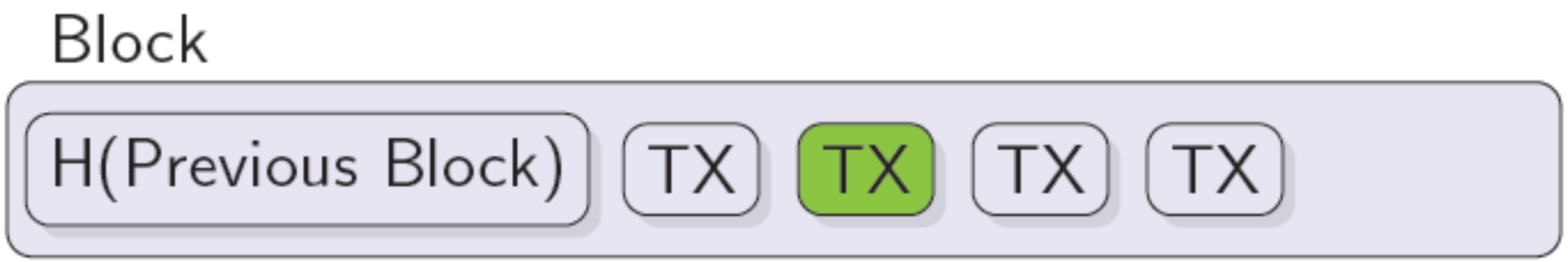
Proof-of-Work

Miner



Proof-of-Work

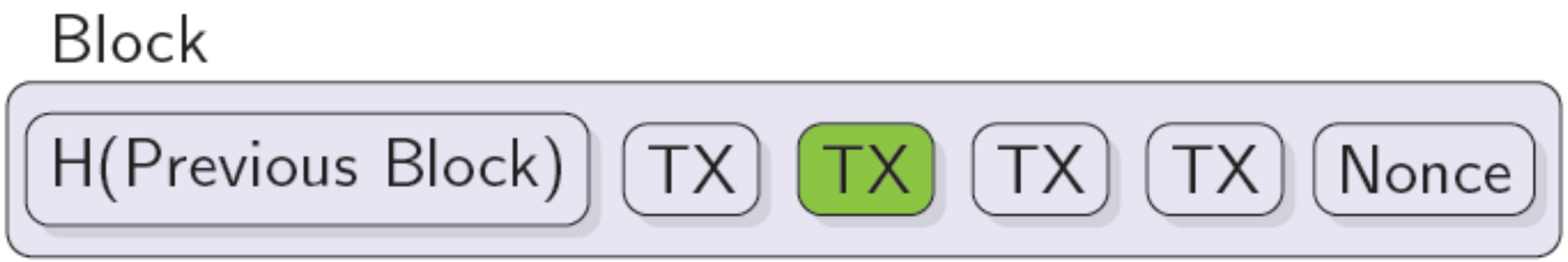
Miner



- H(Block) $\rightarrow$ fd2e2055f117bfa261b5a6c7e11df367...

Proof-of-Work

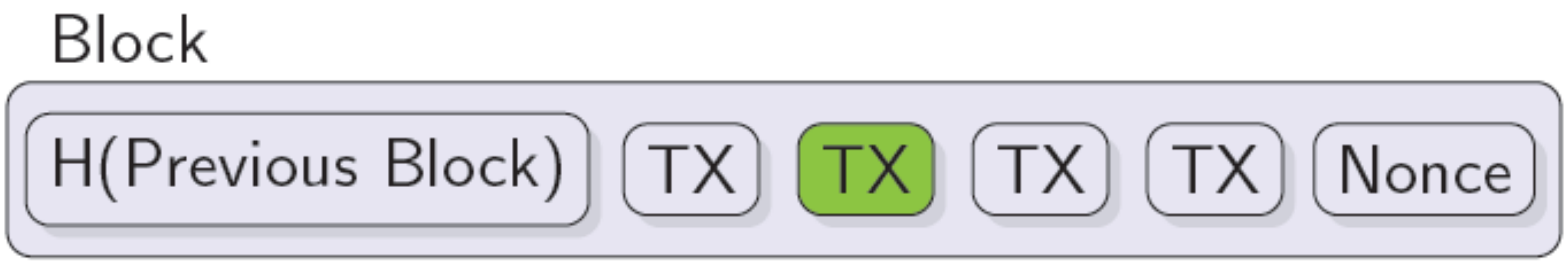
Miner



- $H(\text{Block}|0) \rightarrow$ 094d66aa7c844a9dbb516a41259b5877...

Proof-of-Work

Miner

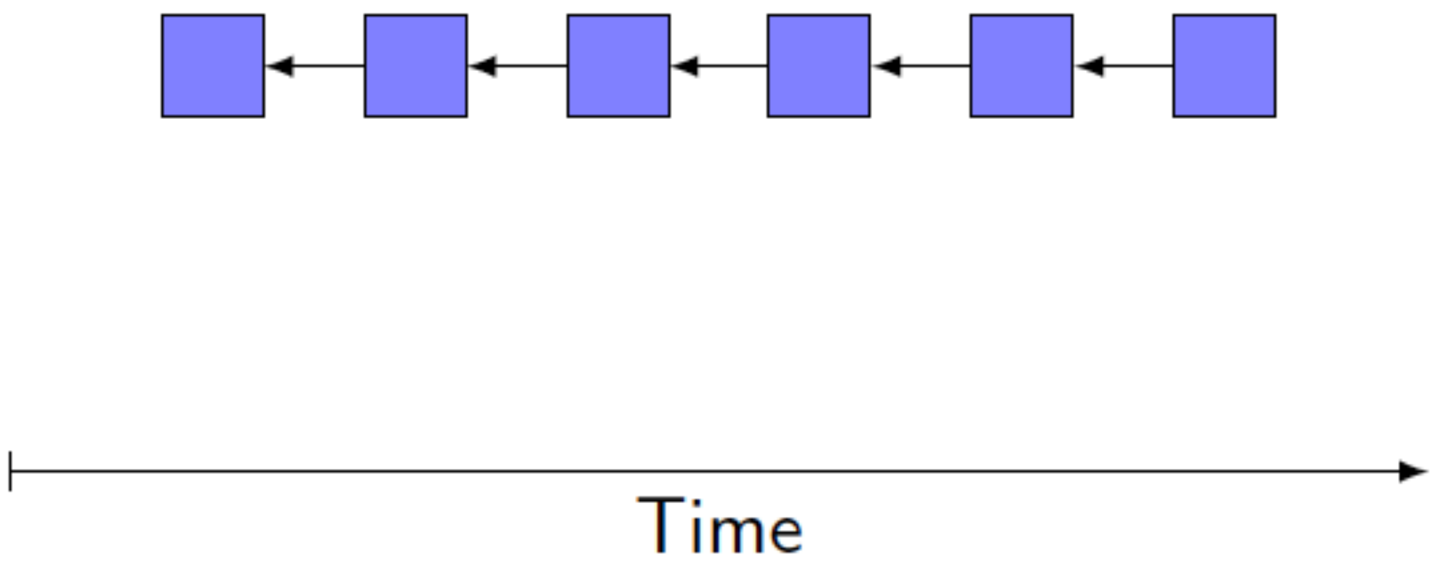


- $H(\text{Block}|0) \rightarrow$ 094d66aa7c844a9dbb516a41259b5877...
- $H(\text{Block}|1) \rightarrow$ f2496854af8bf989171587a9259f634f...
- $H(\text{Block}|2) \rightarrow$ aec87c0ca2e5eb3f23111092f1089ada...
- $H(\text{Block}|3) \rightarrow$ 777f75b2a8ecfdc8026c236fc1d2ffa0...

  $\vdots$

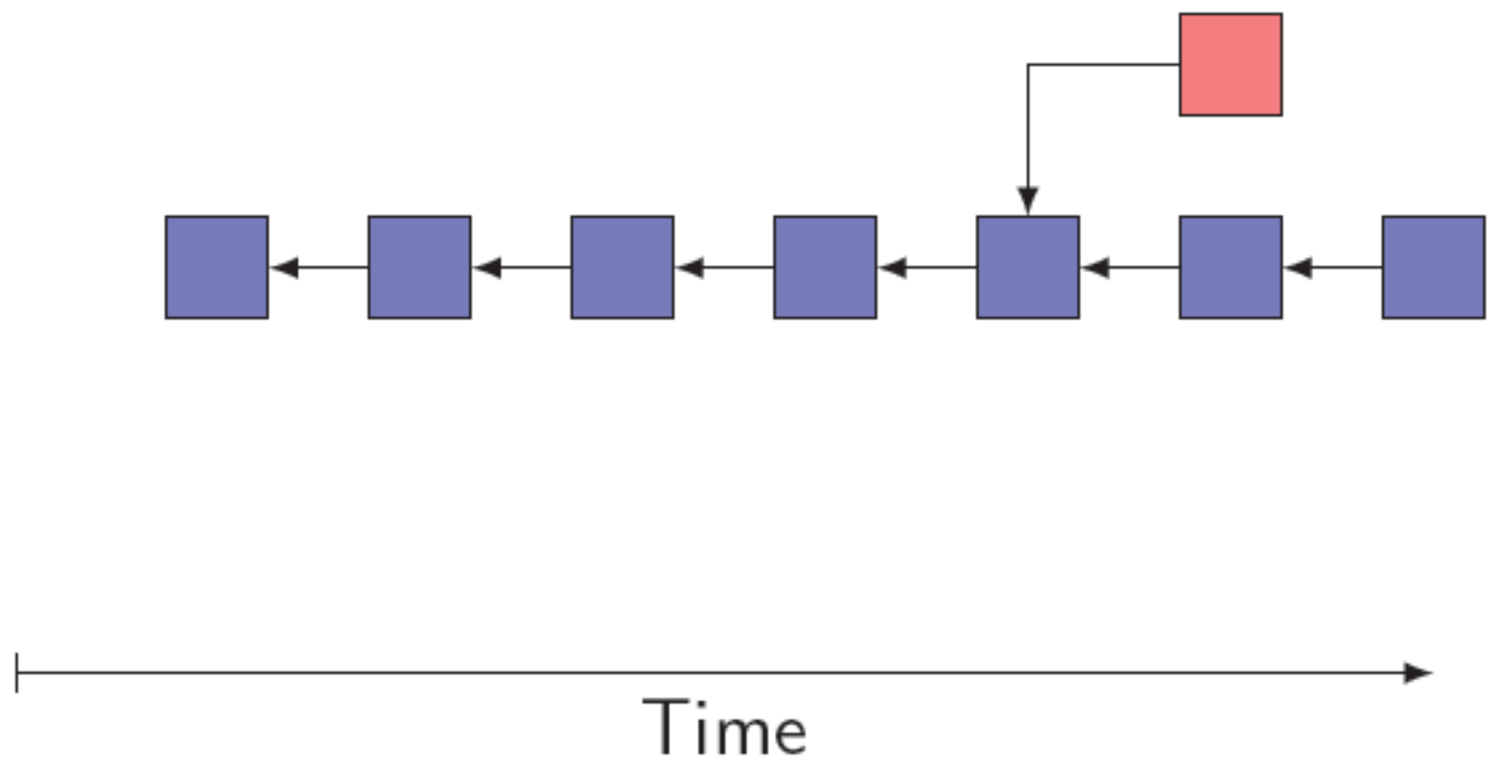
- $H(\text{Block}|961127) \rightarrow$ 000014823419622d4c133672a7d657e...

The Blockchain



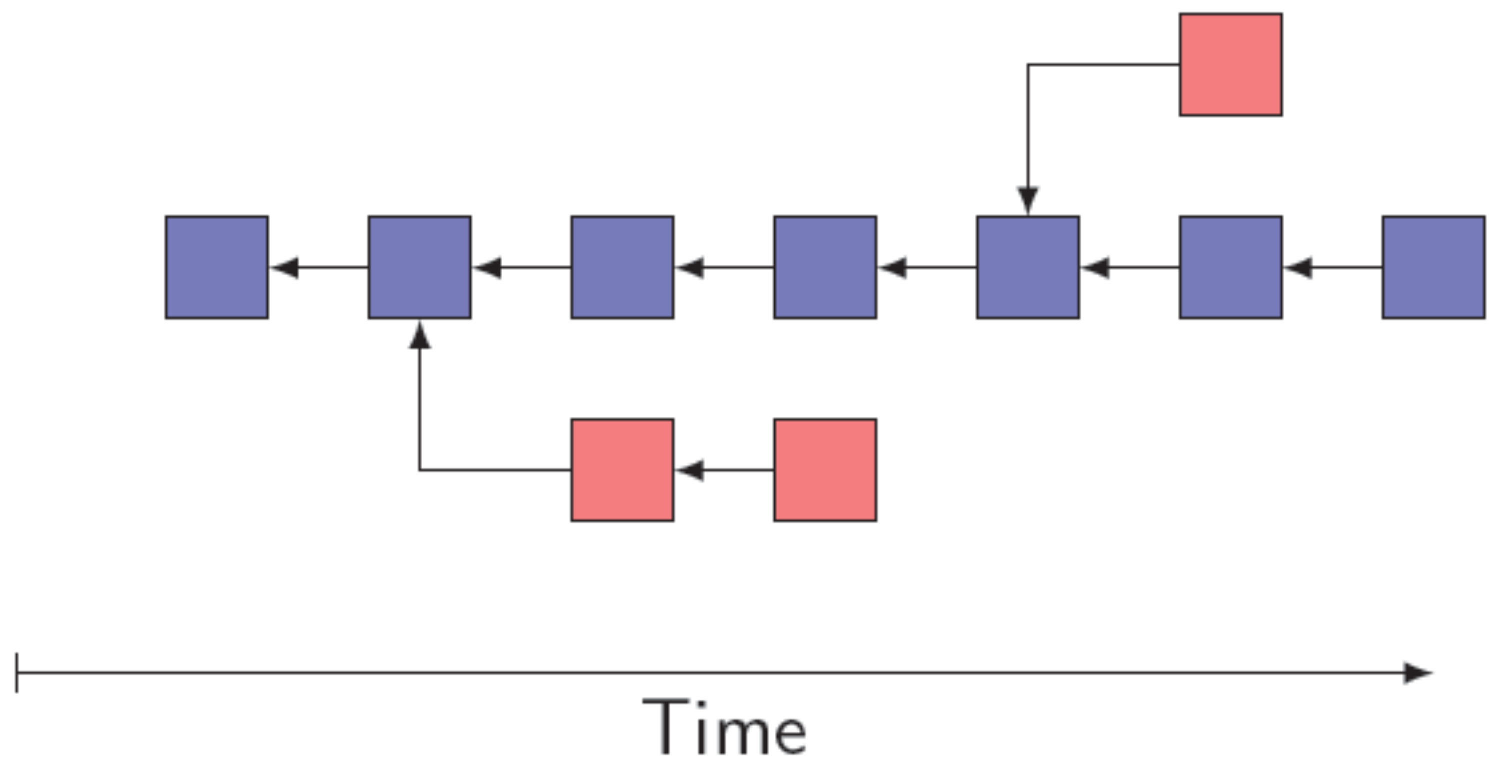
The Blockchain

Miner



The Blockchain

Miner



yes, if 51% computing power is from good miners

Is Bitcoin **stable**?

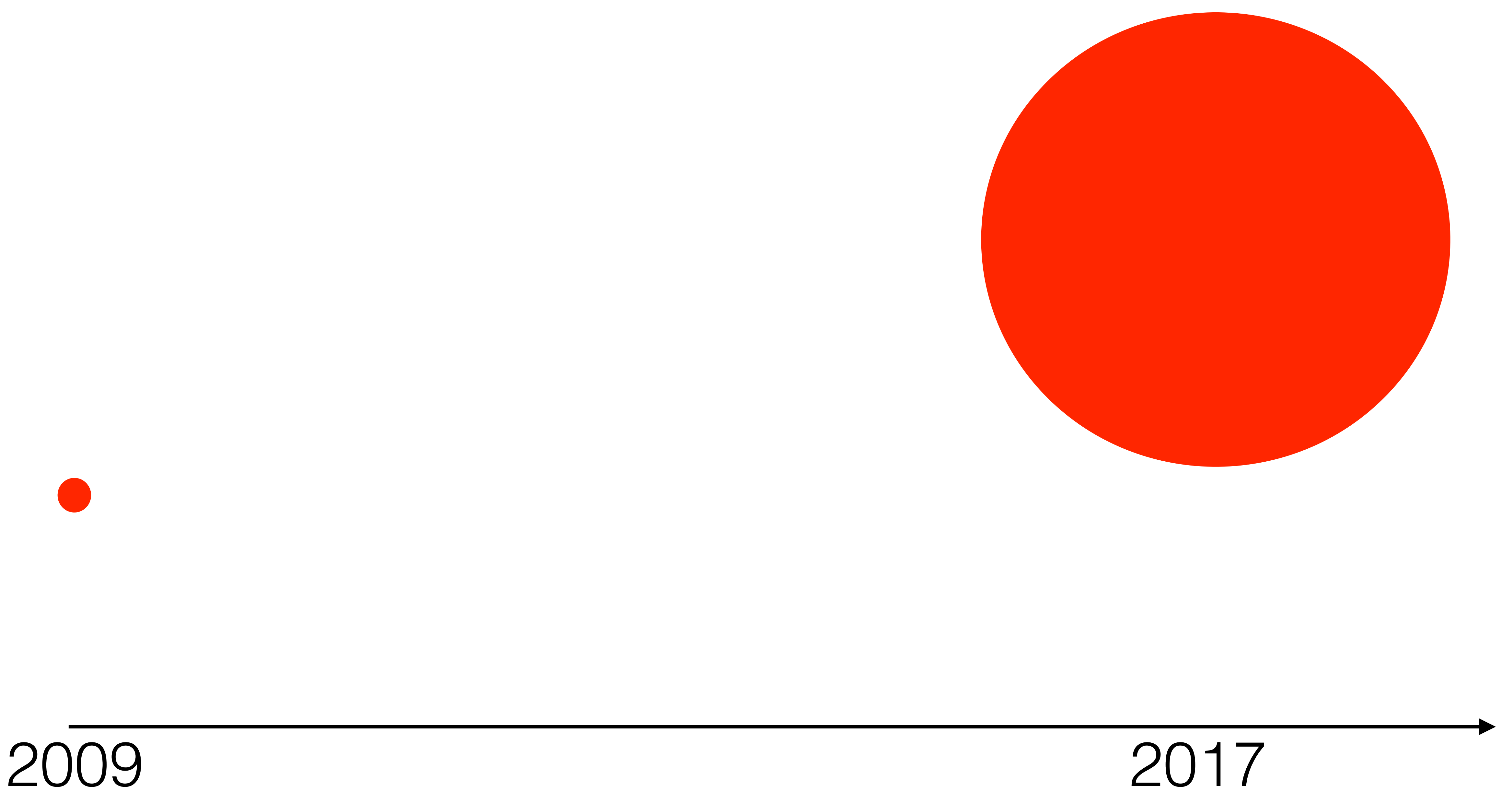
Nakamoto's design

- **Most of tools were known**
  - **Public keys as identities**
  - **Time stamping**
  - **Hash chain**
  - **Incentives**
  - **Proof-of-work**

Nakamoto’s design

- **Amazing design**
  - **Put them together**
- **Cute points**
  - **Open (via PoW); easy to join/leave**
  - **Suitable incentives**
  - **Adaptive difficulty adjustment**
  - **Scalable to a huge network of nodes; very lightweight communication**

Nakamoto’s design

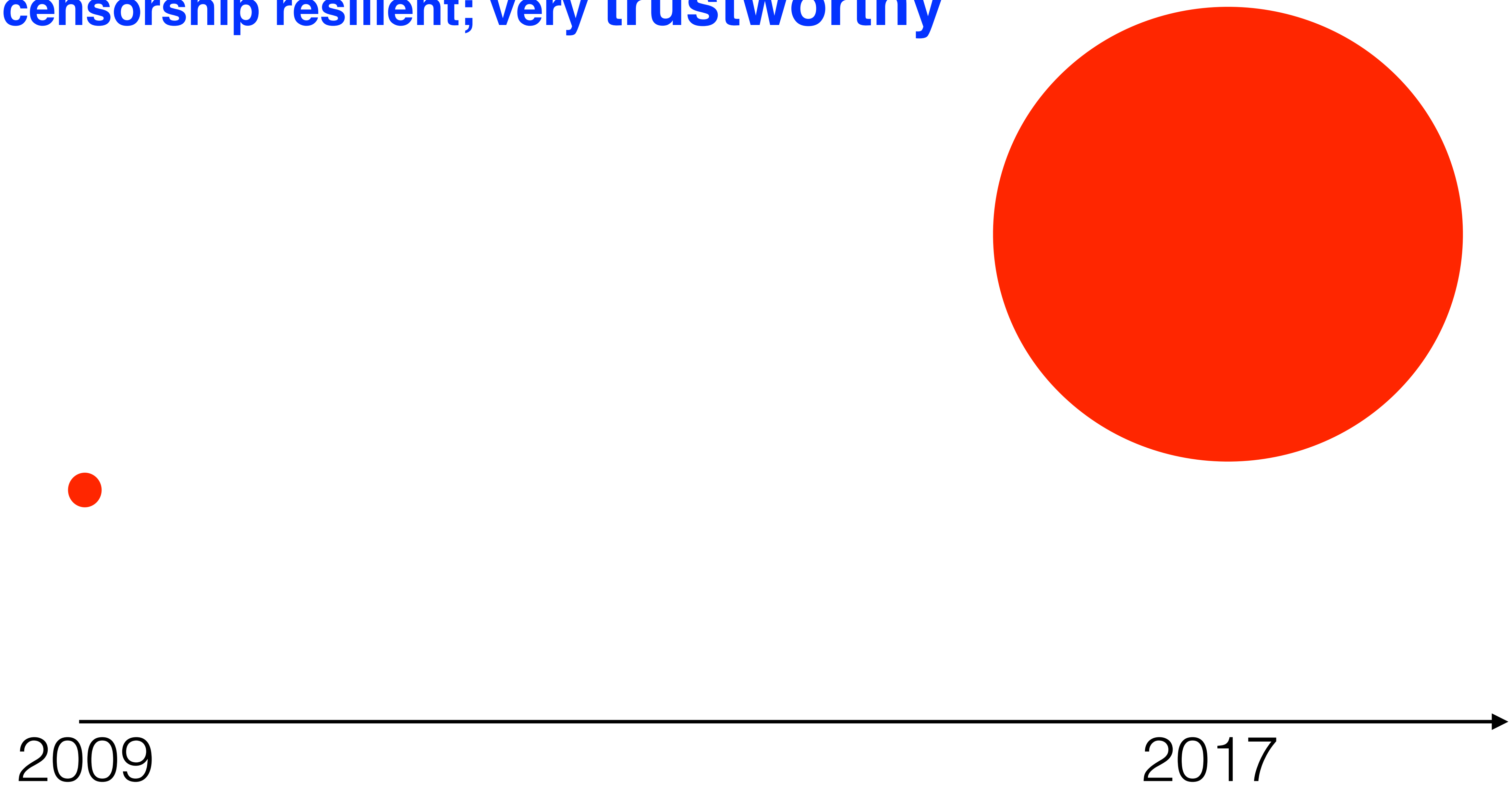


Nakamoto's design

the blockchain is

backed up by a huge network of computing power;

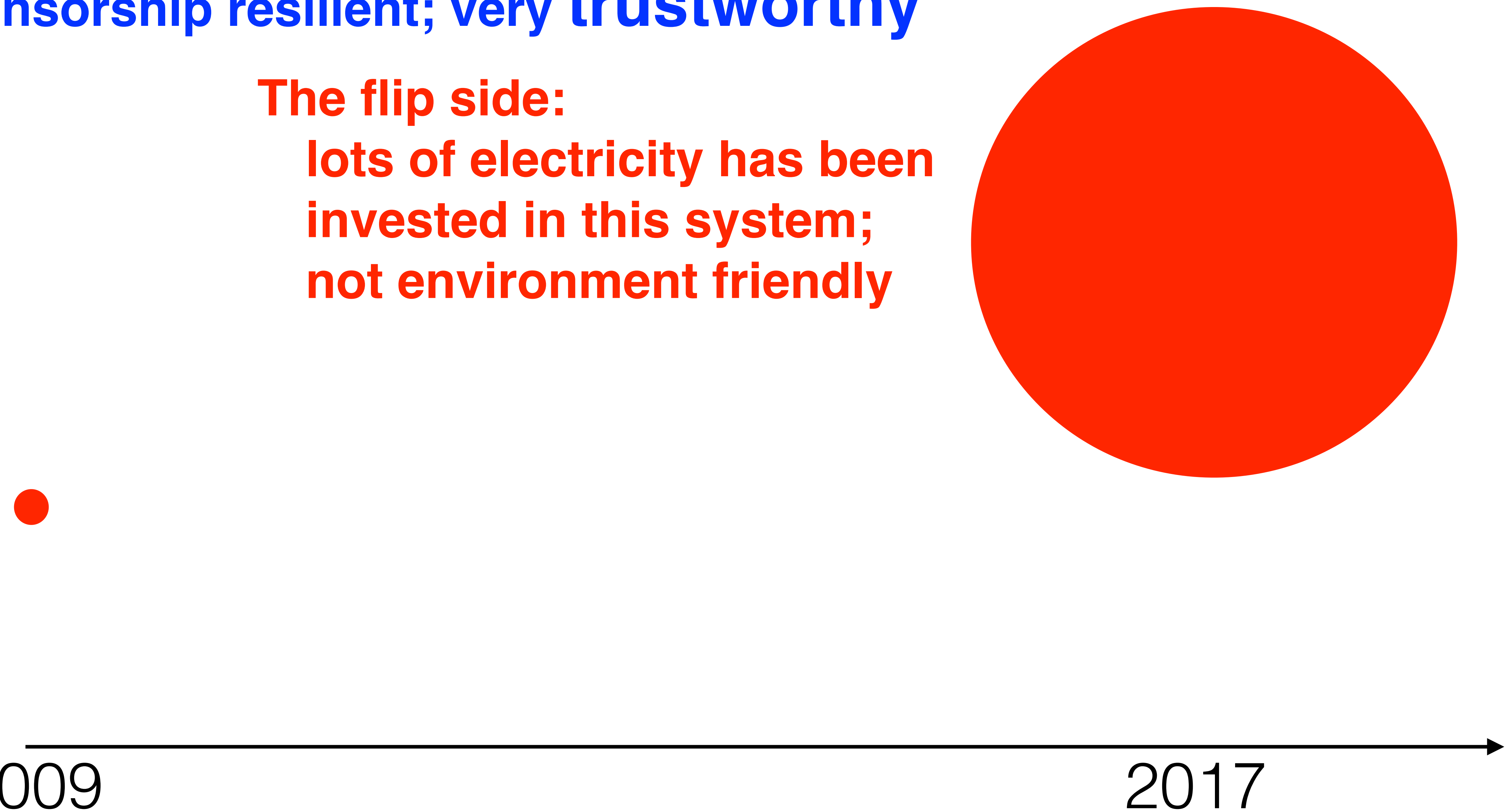
censorship resilient; very trustworthy



Nakamoto's design

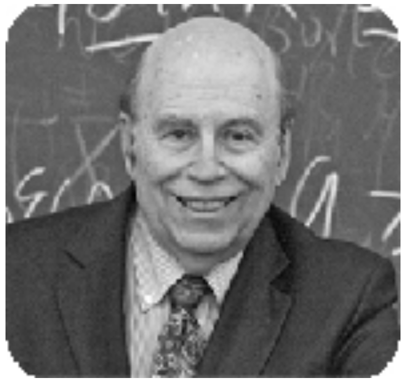
the blockchain is
backed up by a huge network of computing power;
censorship resilient; very trustworthy

The flip side:
lots of electricity has been
invested in this system;
not environment friendly



Cryptographic Foundations

A modern approach to building security systems



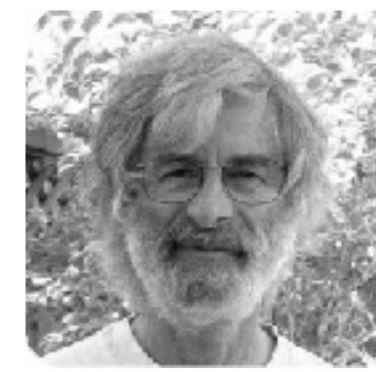
Modern Crypto

Crypto is very successful

We make progresses in multiple directions

- existing territory
- new territory







Crypto Foundations

- the end goal /objective

  syntax and functionality; security properties

- the starting point / building blocks
  what kinds of resources are available

- the construction: connecting the “starting point” and the “end goal”

- the proof: verifying if the connection is sound

- property based paradigm:
  much restricted adversary/environment;
  advantage: much easier to deal with

Property based

vs

Simulation based

- Simulation based paradigm:
  complex adversary/environment
  advantage: much easier to use

Nakamoto's Protocol: The Simplified version

Defining the ledger objective

[Garay, Kiayias, Leonardos 14]

imagine that time is divided in rounds

and protocol organizes transactions in a sequence of blocks

Persistence: parameter *k*. If an honest party reports a transaction tx as "stable" (>*k* blocks deep) then, whenever an honest party reports it as stable, it will be in the same position

Liveness: parameters *u*, *k*. If all honest parties attempt to insert the transaction *tx* in the ledger, then, after *u rounds*, all honest parties will report it as stable (>*k* blocks deep) and will always do so

transaction processing time : *u* as a function of *k*

Garay, Kiayias, Leonardos, The Bitcoin Backbone Protocol: Analysis and Applications. Eurocrypt 2015, IACR ePrint 2014

The Bitcoin Backbone Protocol

[Garay, Kiayias, Leonardos 14]

- An abstraction based on the Bitcoin implementation.

  - **Importantly** : it distinguishes between data structure (blockchain) and application layer (transactions).

Main Loop

[Garay, Kiayias, Leonardos 14]

$\mathcal{C} \leftarrow \varepsilon$
$\mathit{state} \leftarrow \varepsilon$
$\mathit{round} \leftarrow 0$
while $\textsc{True}$ **do**
 $\widetilde{\mathcal{C}} \leftarrow \mathsf{maxvalid}(\mathcal{C}, \text{all chains found in } \textsc{Receive}())$
 $\langle \mathit{state}, x \rangle \leftarrow I(\mathit{state}, \widetilde{\mathcal{C}}, \mathit{round}, \textsc{Input}(), \textsc{Receive}())$ ▷ Determine the x-value.
 $\mathcal{C}_{\mathsf{new}} \leftarrow \mathsf{pow}(x, \widetilde{\mathcal{C}})$
 if $\mathcal{C} \neq \mathcal{C}_{\mathsf{new}}$ **then**
  $\mathcal{C} \leftarrow \mathcal{C}_{\mathsf{new}}$
  $\textsc{Broadcast}(\mathcal{C})$
 end if
 $\mathit{round} \leftarrow \mathit{round} + 1$
 if $\textsc{Input}()$ contains $\textsc{Read}$ **then**
  write $R(\mathbf{x}_{\mathcal{C}})$ to $\textsc{Output}()$
 end if
end while

Backbone Protocol Properties

Common Prefix

(informally)

If two players prune a sufficient number of blocks from their chains they will obtain the same prefix

Chain Quality

(informally)

Any (large enough) chunk of an honest player's chain will contain some blocks from honest players

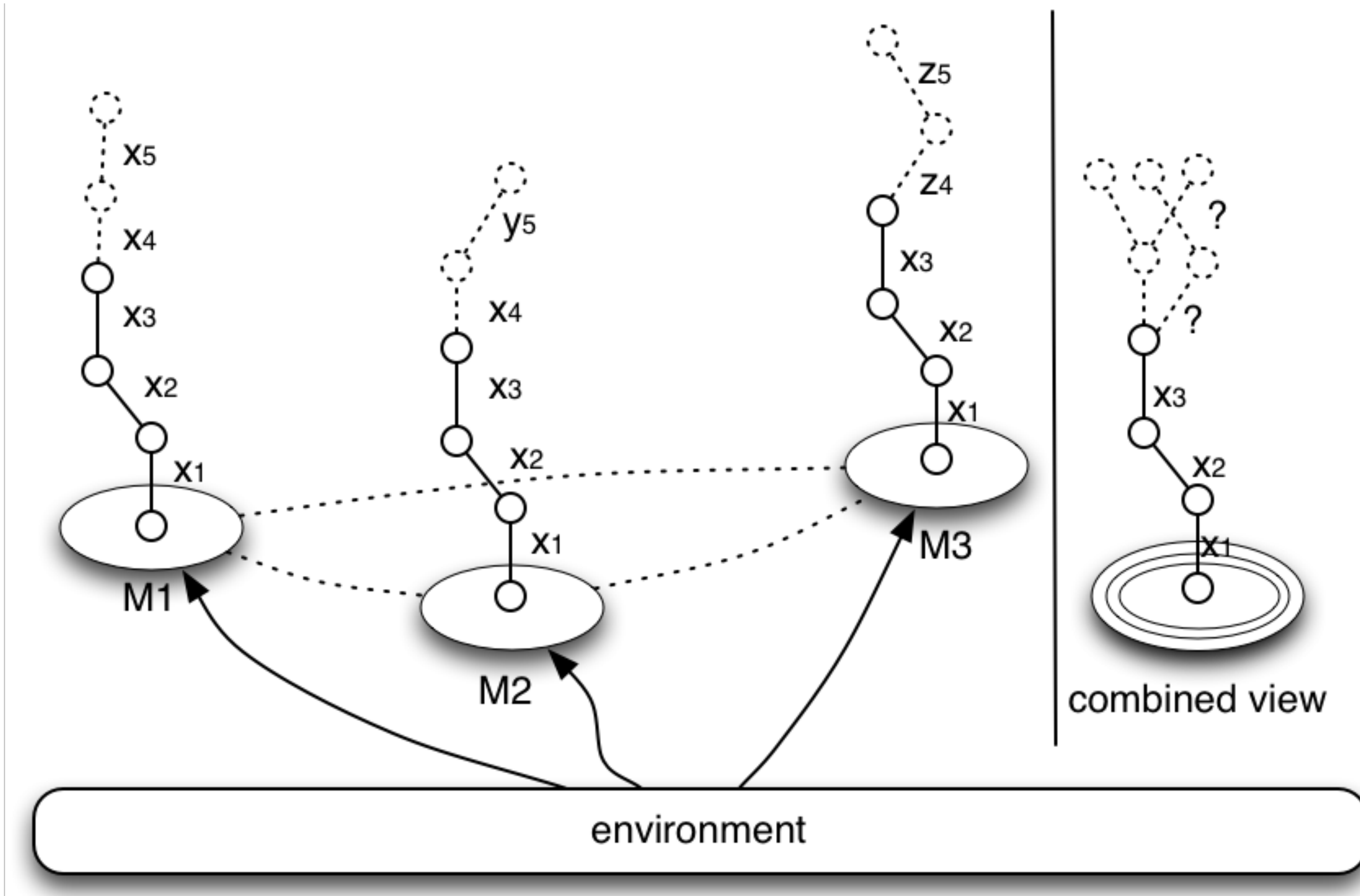
Chain Growth

(informally)

the chain of any honest player grows at least at a steady rate - the chain speed coefficient

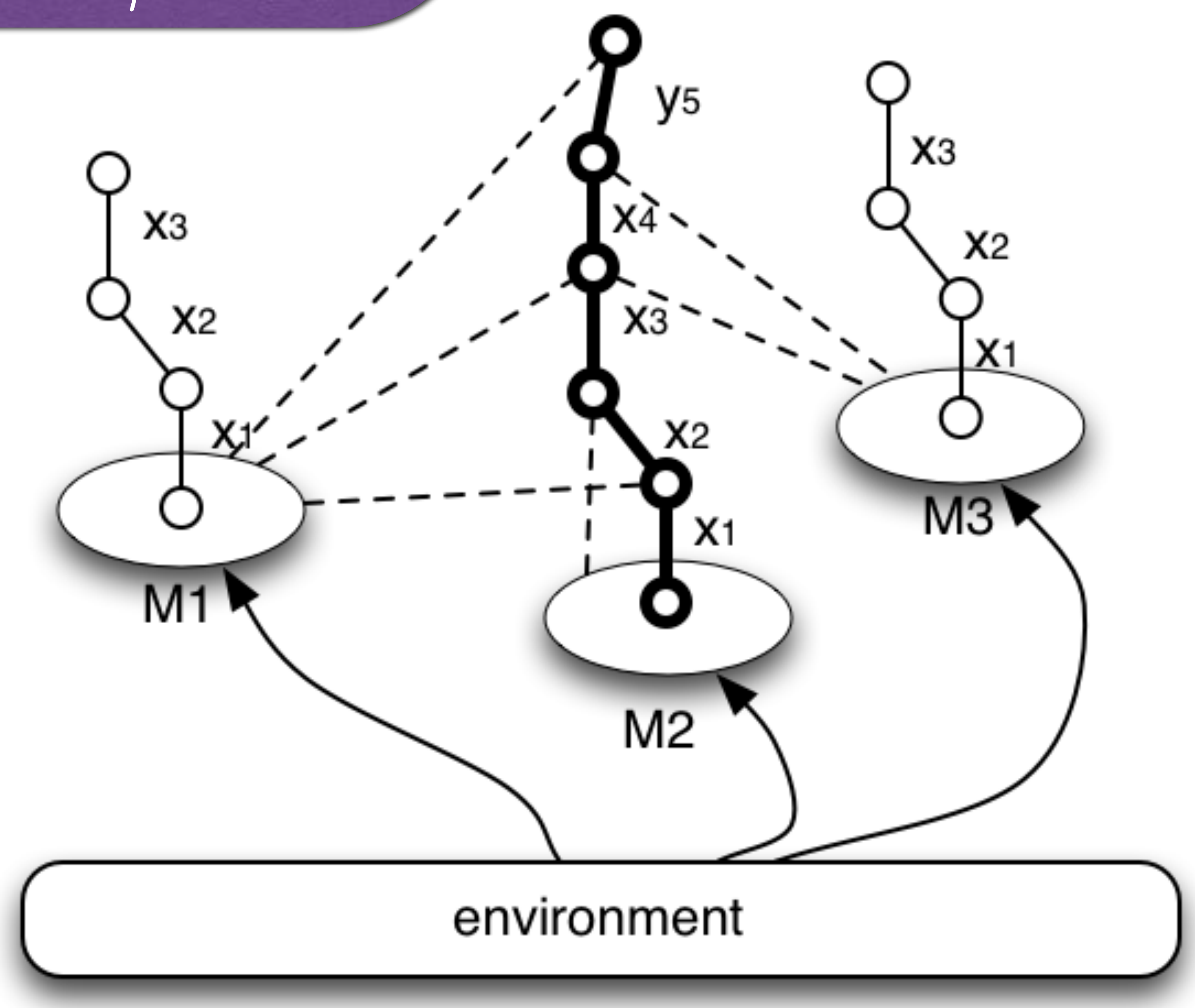
CP: will honest players converge?

$\forall r_1, r_2, (r_1 \le r_2), P_1, P_2,$ with $\mathcal{C}_1, \mathcal{C}_2 :\ \mathcal{C}_1^{\lceil k} \preceq \mathcal{C}_2$



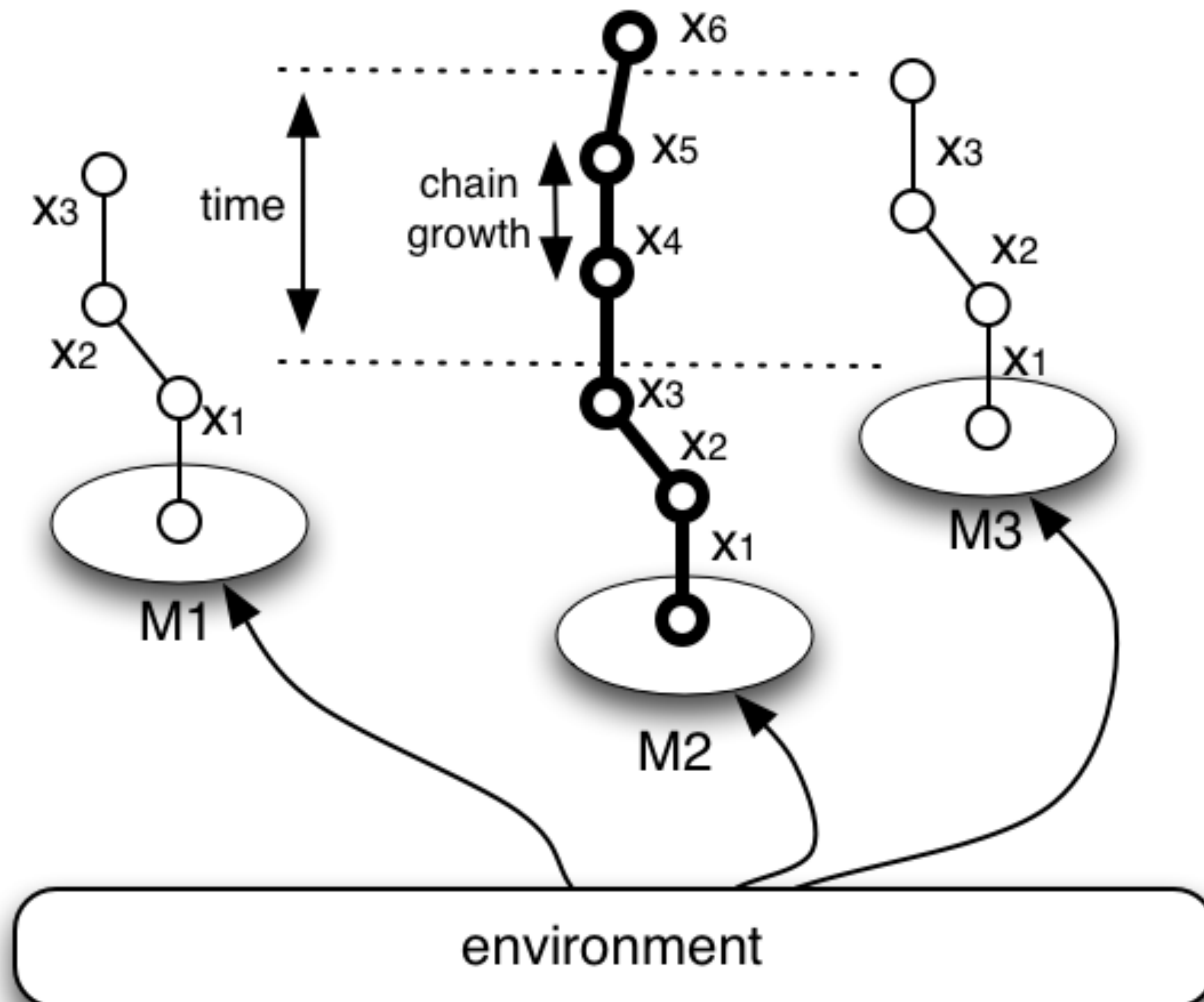
CQ: are honest blocks going to be adopted by the parties?

Parameters $\mu \in (0,1), k \in \mathbb{N}$
The proportion of blocks in any k-long subsequence produced by the adversary is less than μk



Chain Growth: does the chain grow?

Parameters $\tau \in (0,1), s \in \mathbb{N}$
$\forall r_1, r_2$ honest player P with chains $\mathcal{C}_1, \mathcal{C}_2$
$r_2 - r_1 \geq s \implies |\mathcal{C}_2| - |\mathcal{C}_1| \geq \tau s$



Nakamoto's Protocol: The Full-fledged version

Can we have a
complete analysis ?

several progresses for analyzing the simplified Nakamoto protocol

- Pass et al, Eurocrypt 17, more realistic network
- Garay et al, Crypto17, adaptive difficulty adjustment
- What are missing ?

Pass, Seeman, Shelat, *Analysis of the Blockchain Protocol in Asynchronous Networks*. Eurocrypt 2017.
Garay, Kiayias, Leonardos, *The Bitcoin Backbone Protocol with Chains of Variable Difficulty*. Crypto 2017.

Multi-mode systems

[Duong, **Z**, Chepurnoy 17]

- Full mode
- light modes (SPV, prune,…)
- Bitcoin is a multi-mode system by design

Duong, Zhou, Chepurnoy, *Multi-Mode Cryptocurrency Systems*. Manuscript.

Multi-mode systems

[Duong, **Z**, Chepurnoy 17]

- Why multi-mode ?

- How to define the security?

Duong, Zhou, Chepurnoy, *Multi-Mode Cryptocurrency Systems*. Manuscript.

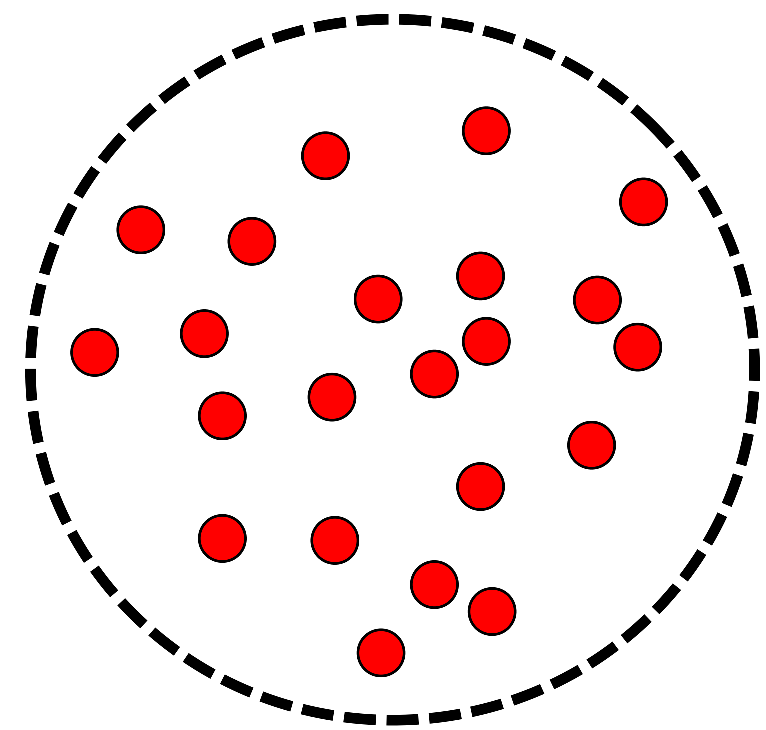
Alternative Mechanisms

A Unified View

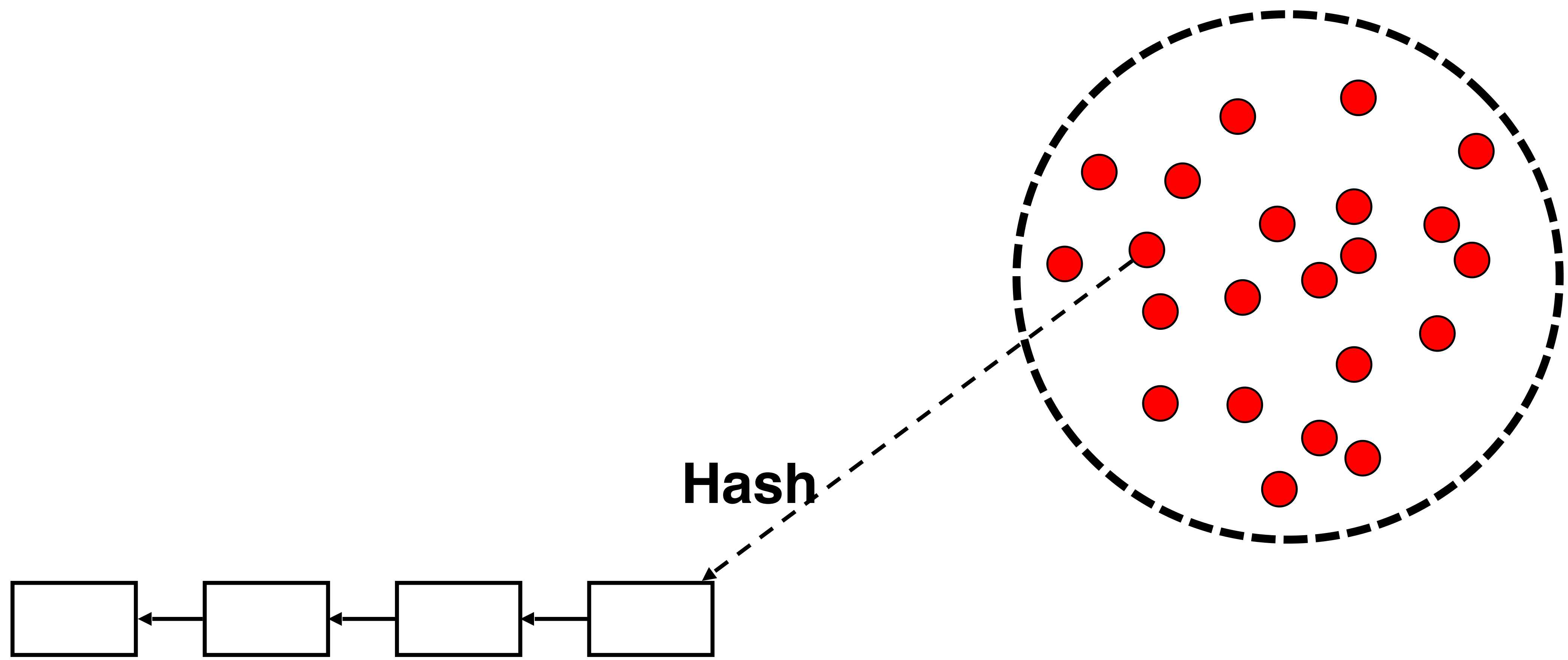
We don't want to put all eggs in one basket.

Can we do a better job than Nakamoto?

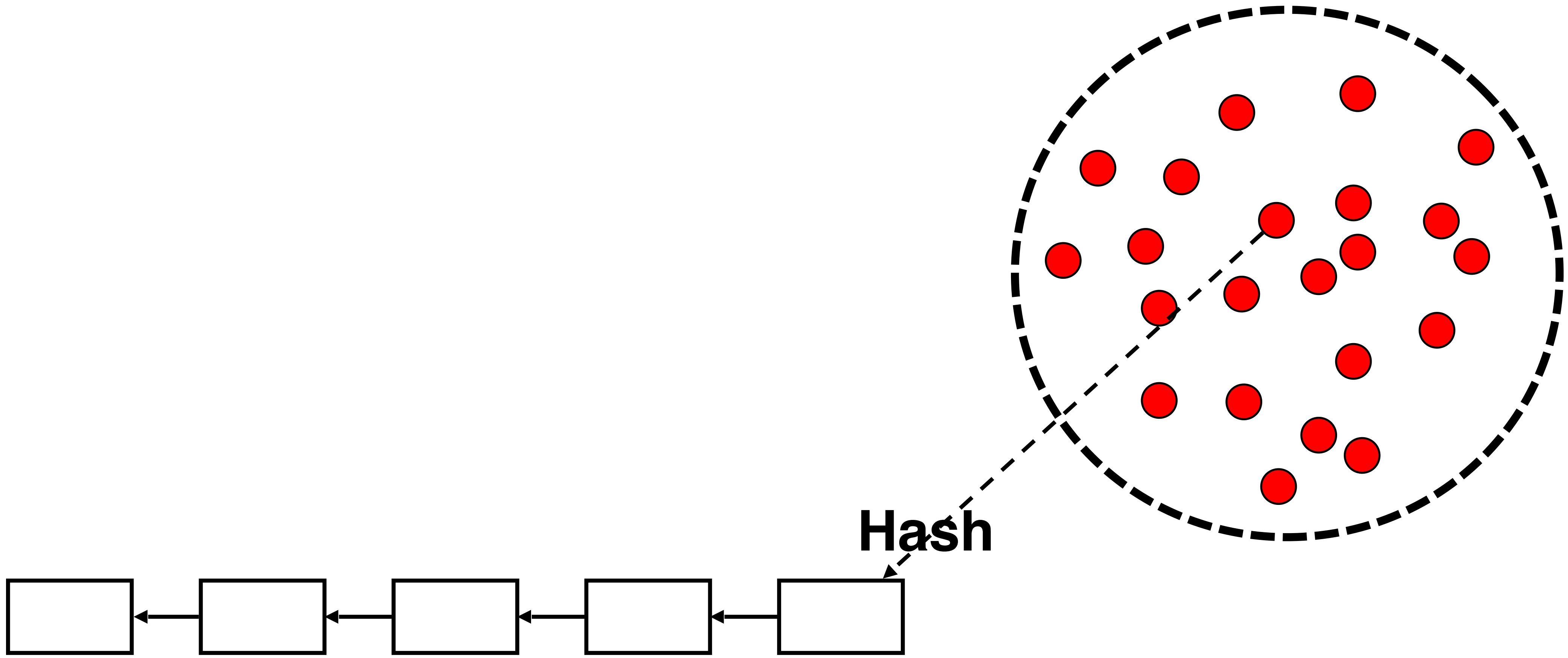
Nakamoto's design



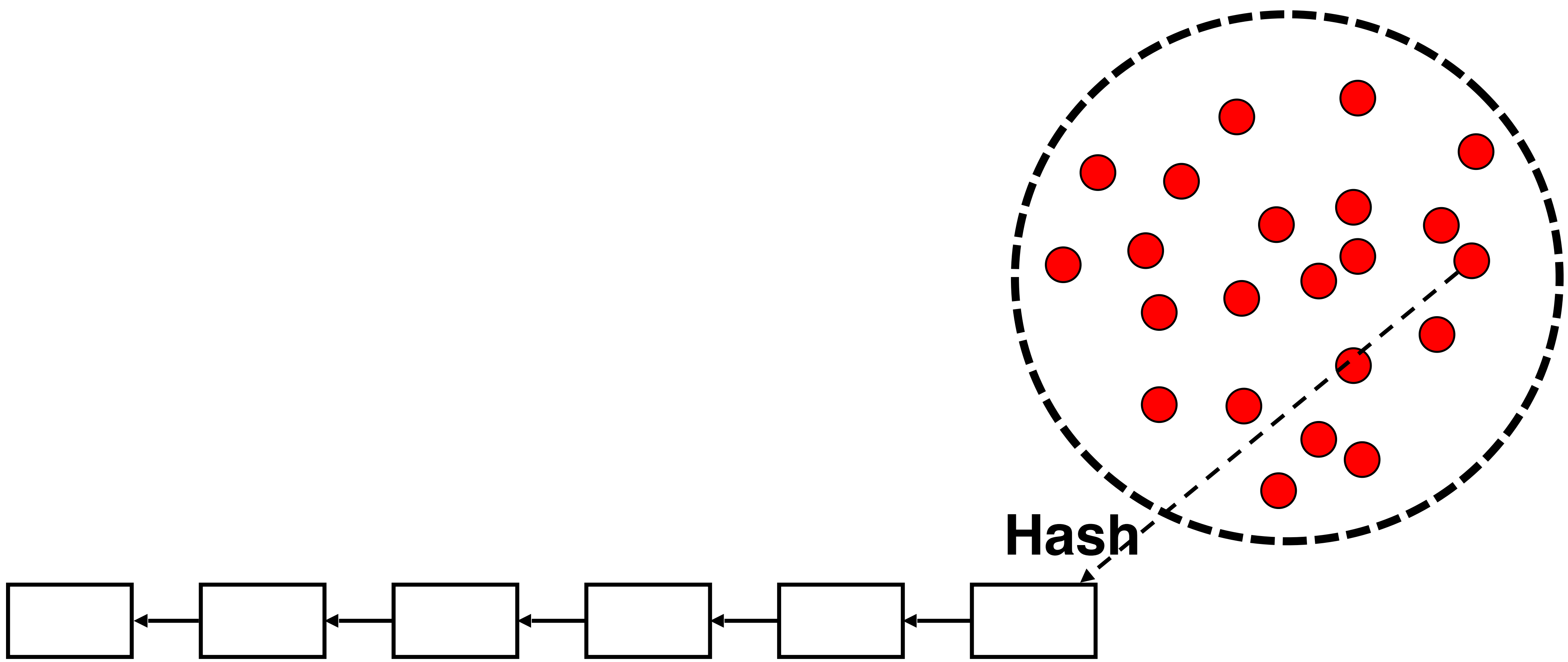
Nakamoto’s design



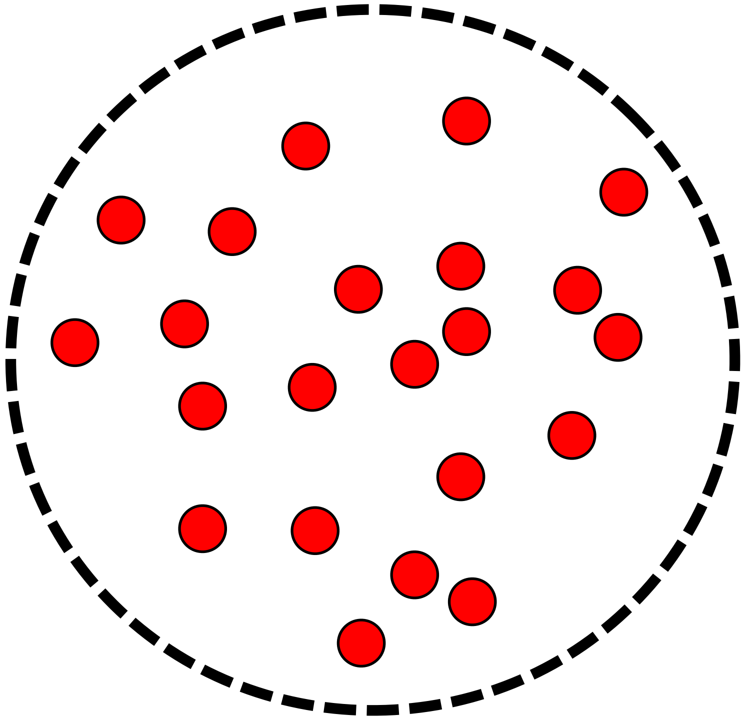
Nakamoto's design



Nakamoto's design



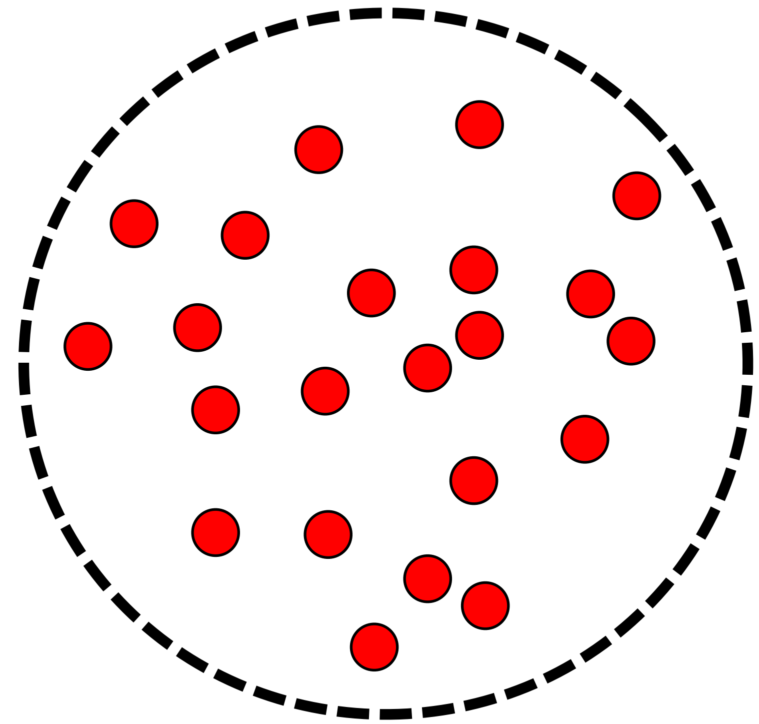
Nakamoto's design



Alternative View

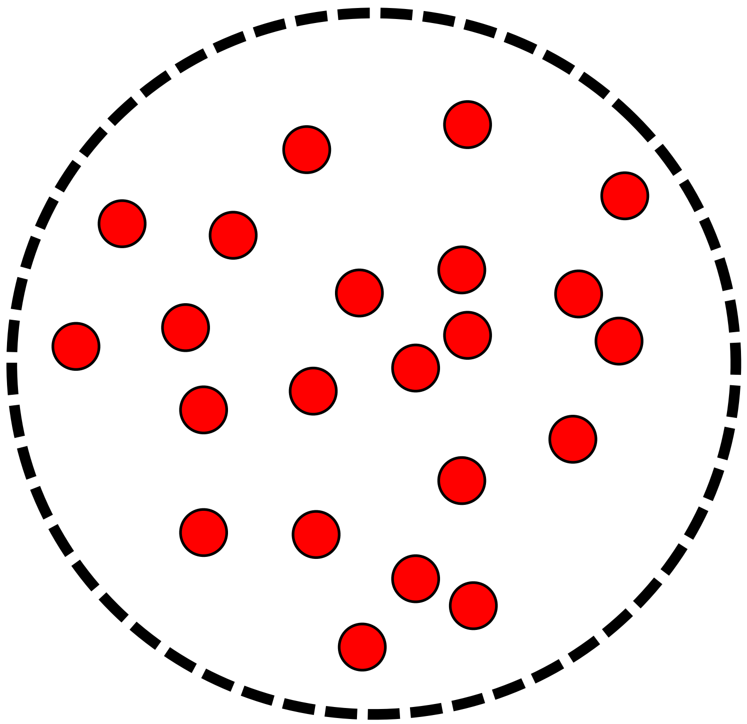
Nakamoto’s design

(inspired by ideas in [Garay, Kiayias, **Z**., CSF10])

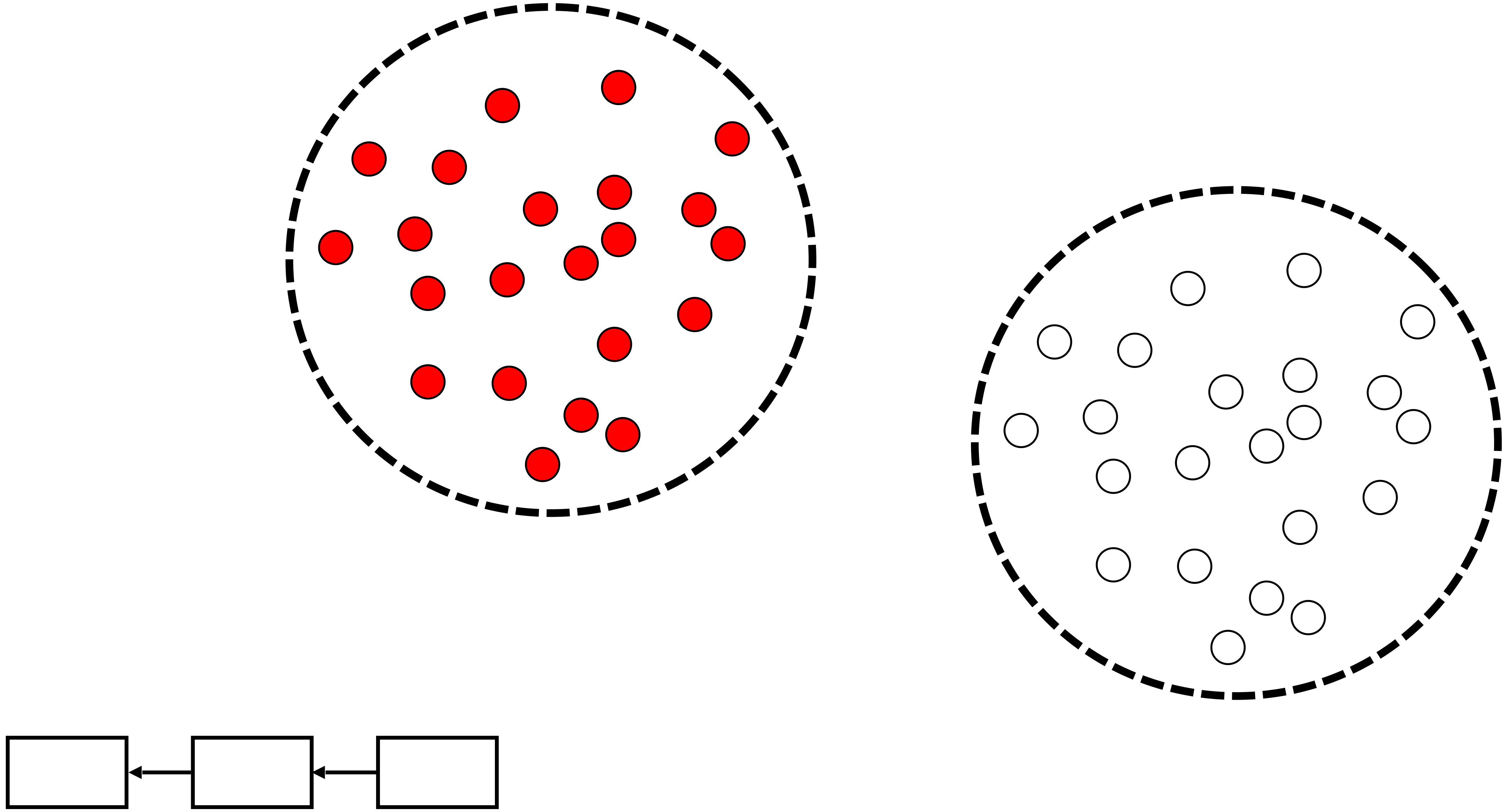


Garay, Kiayias, Zhou, A Framework for the Sound Specification of Cryptographic Tasks. CSF 2010

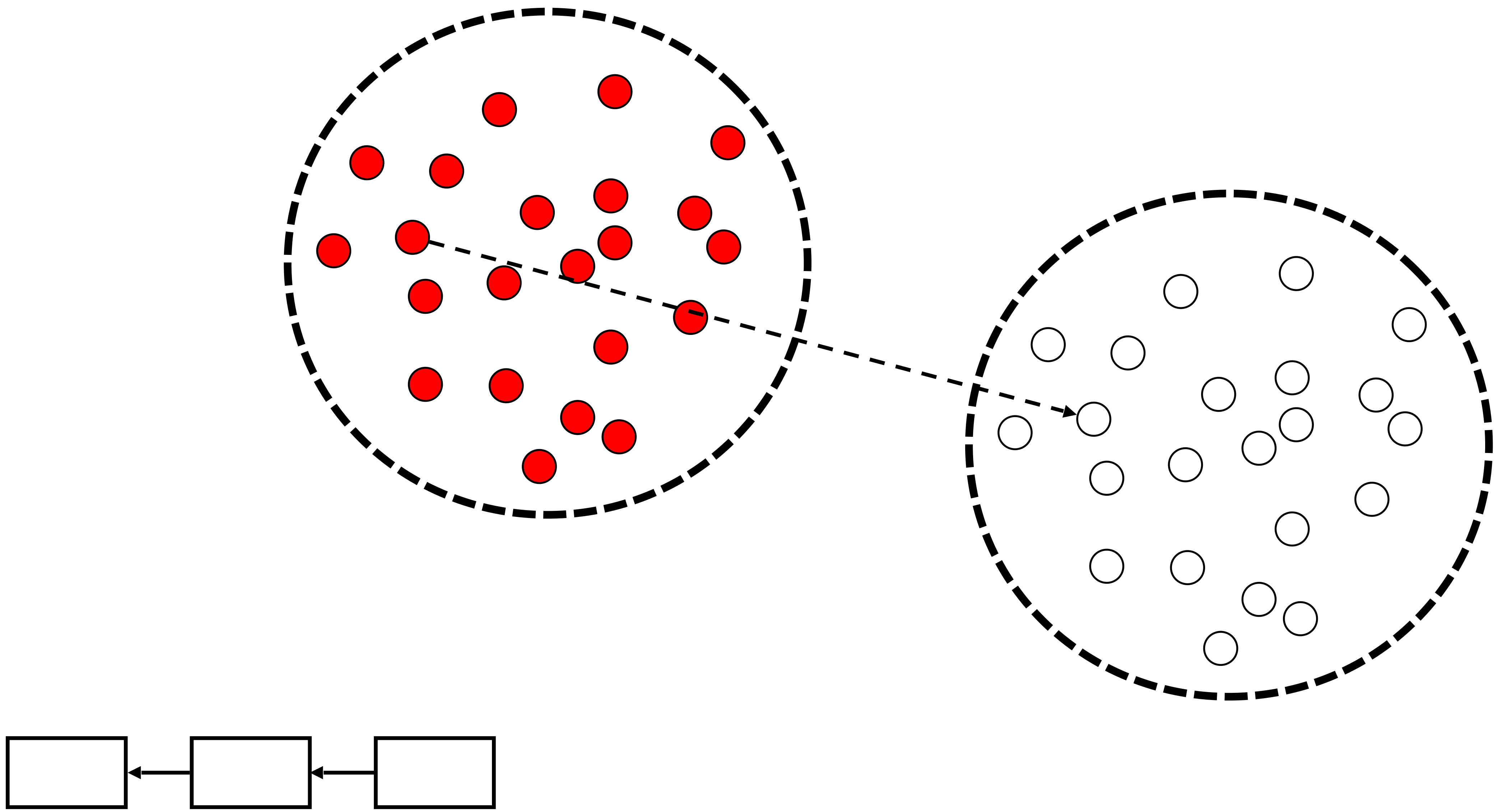
Nakamoto Blockchain: Alternative View



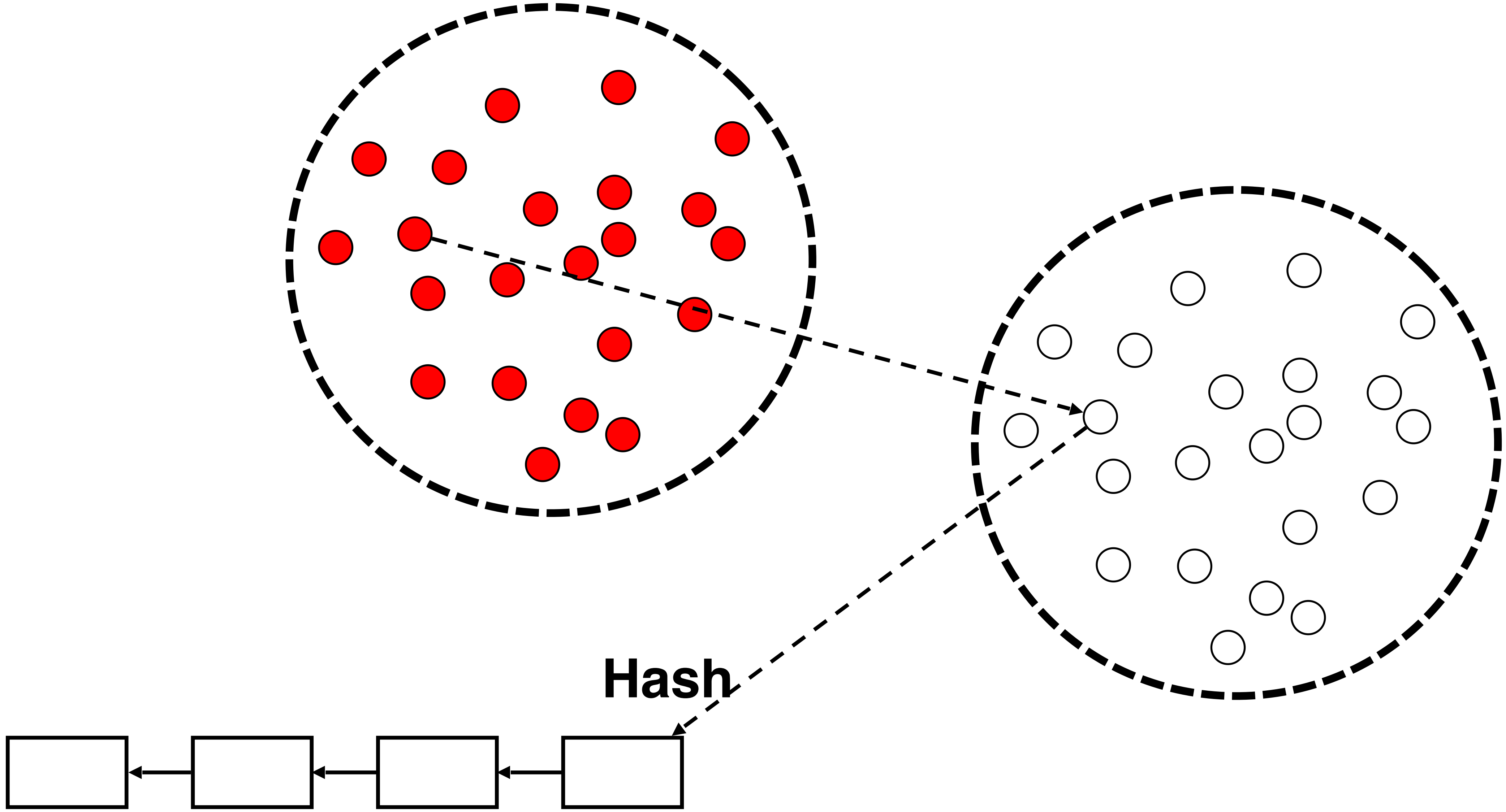
Nakamoto Blockchain: Alternative View



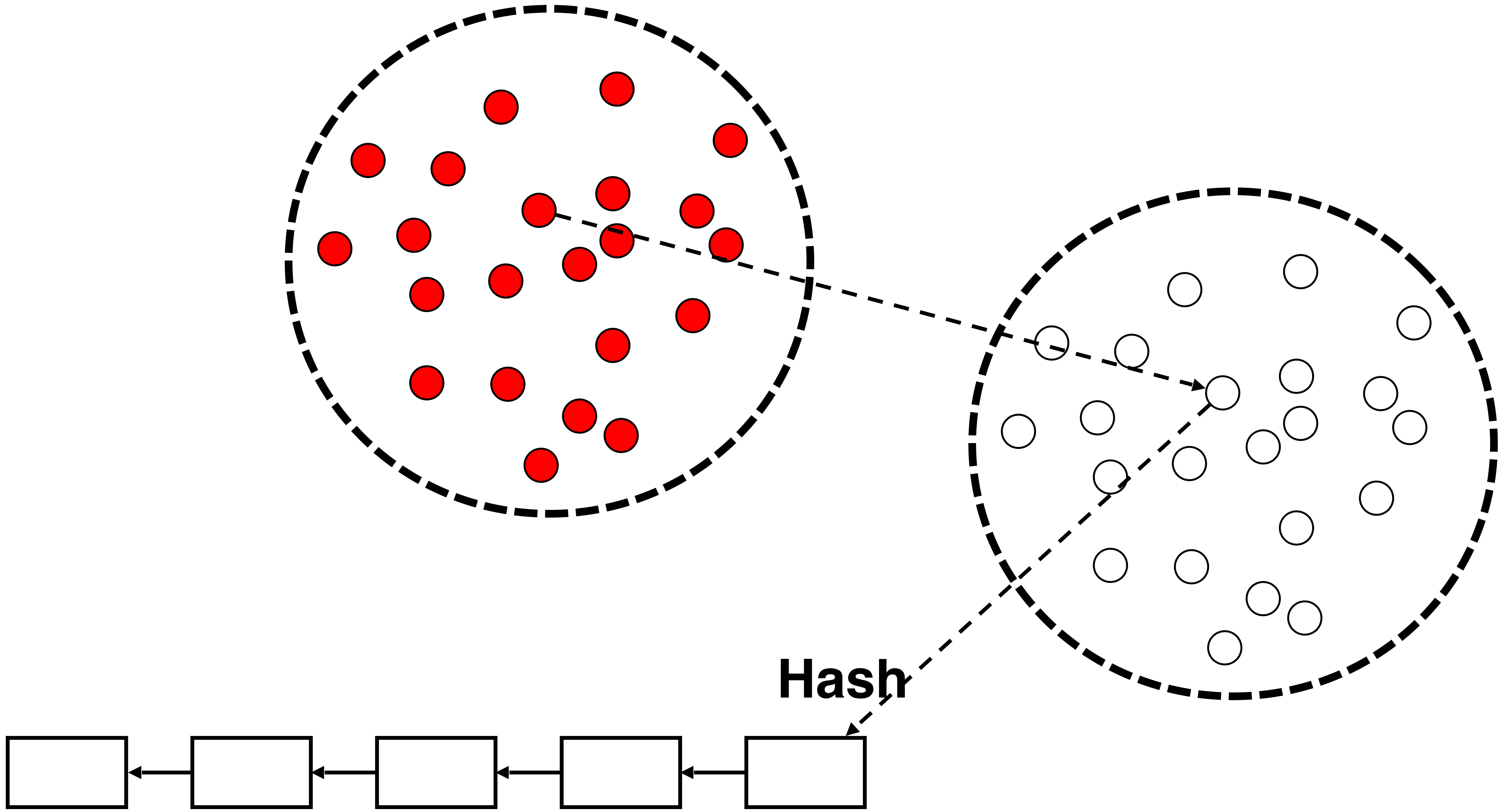
Nakamoto Blockchain: Alternative View



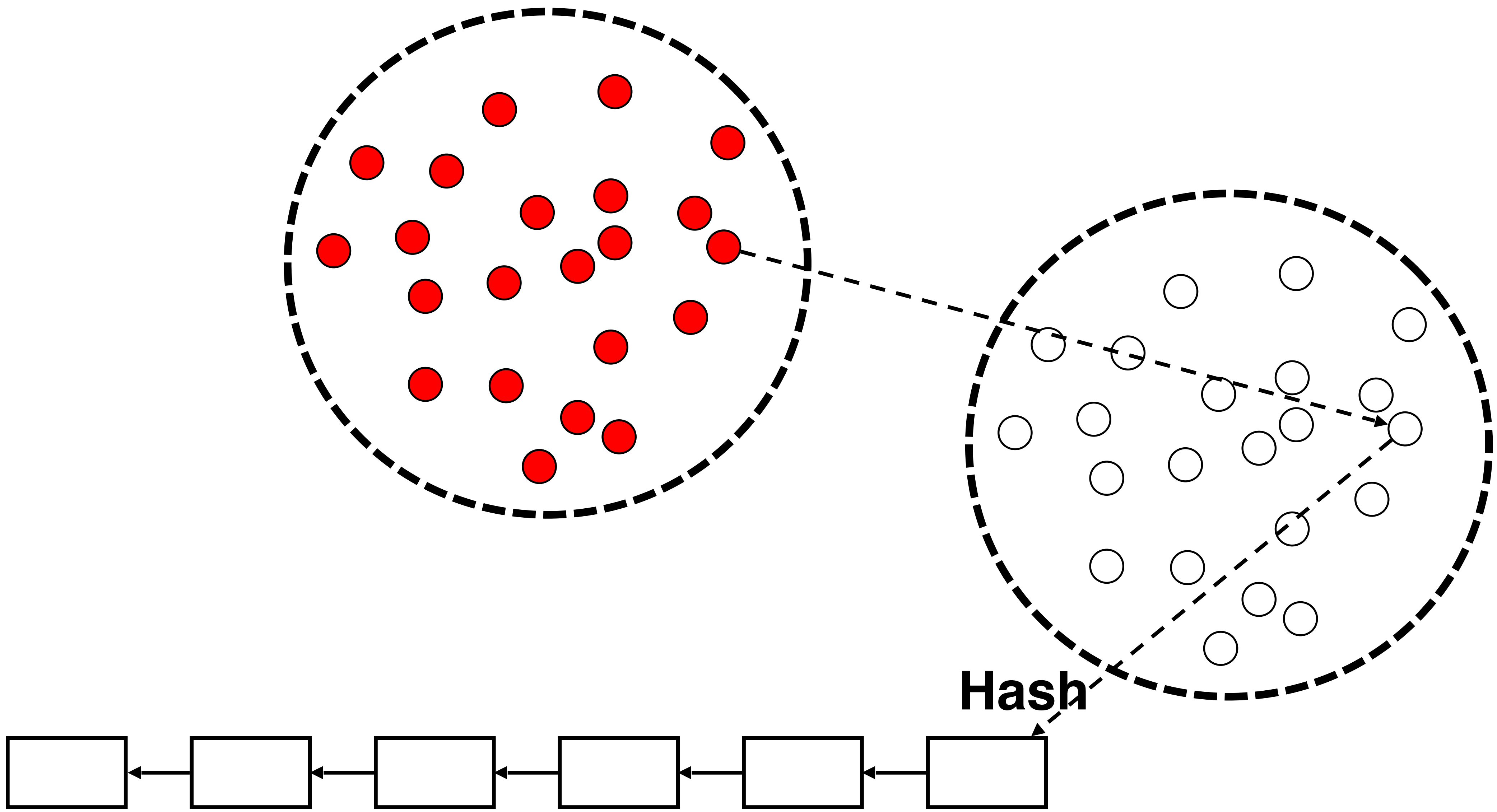
Nakamoto Blockchain: Alternative View



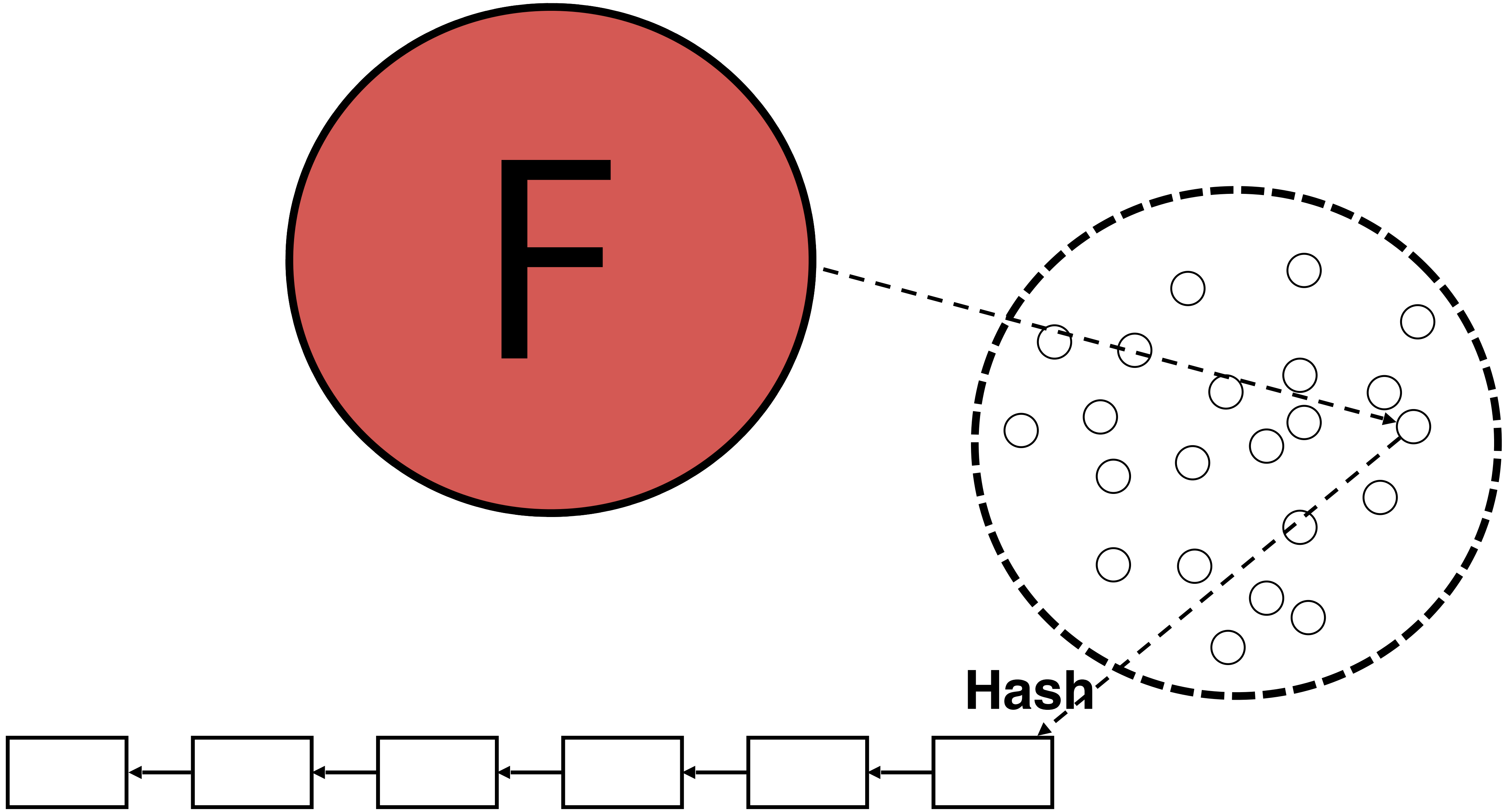
Nakamoto Blockchain: Alternative View

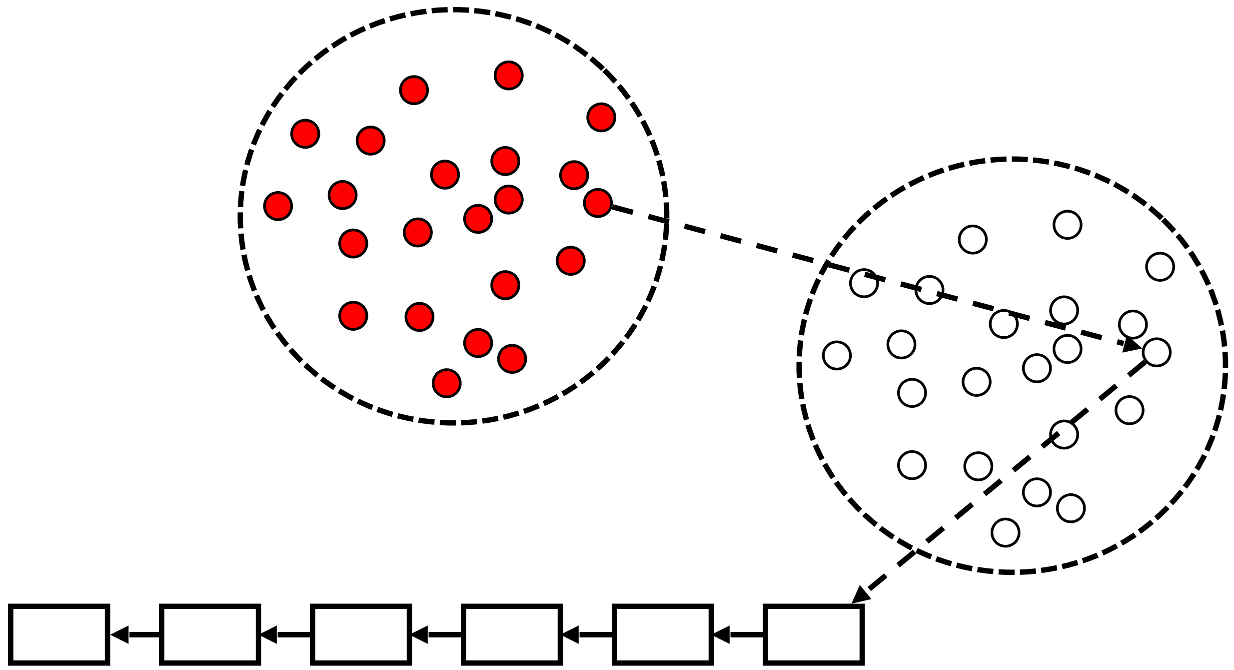


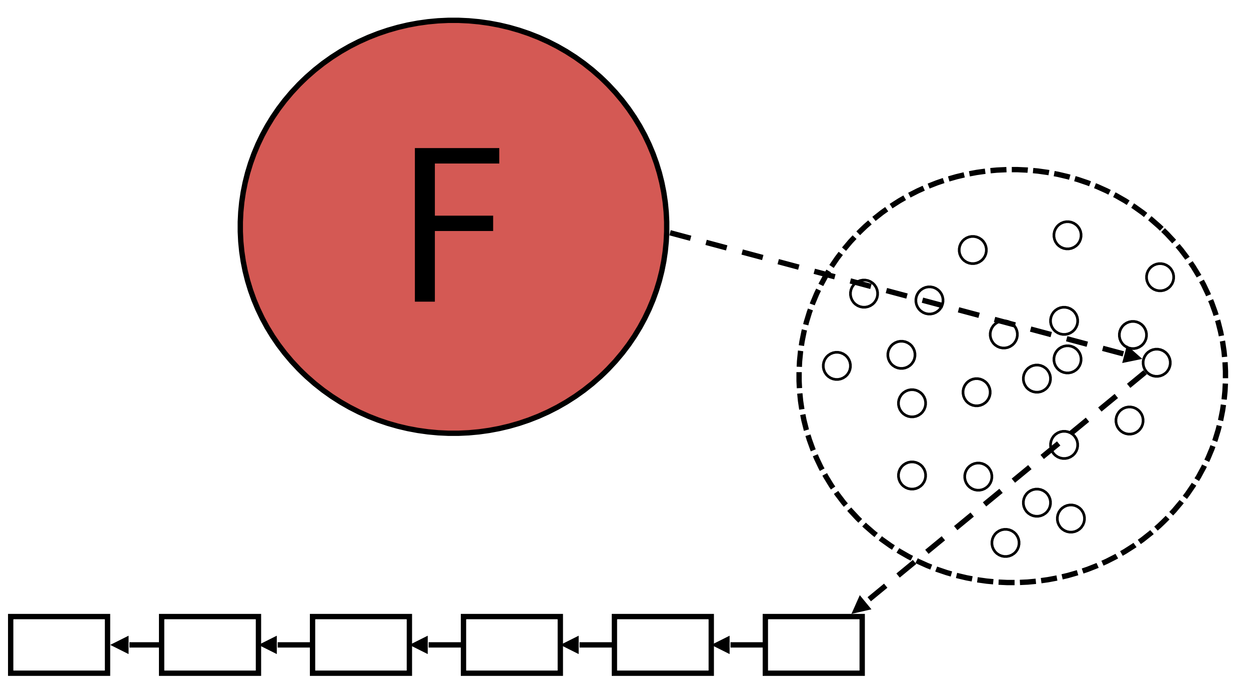
Nakamoto Blockchain: Alternative View



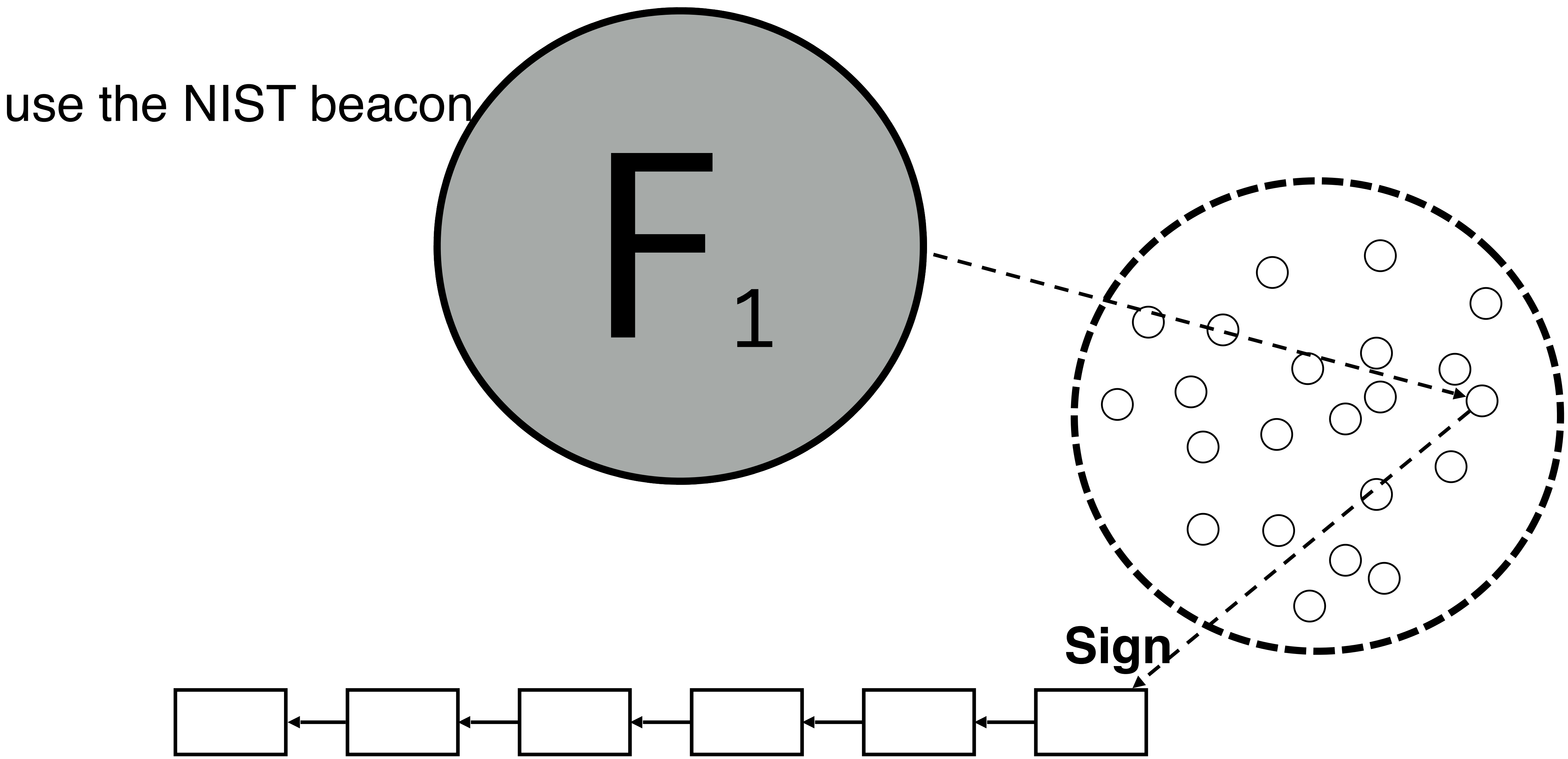
Nakamoto Blockchain: Alternative View





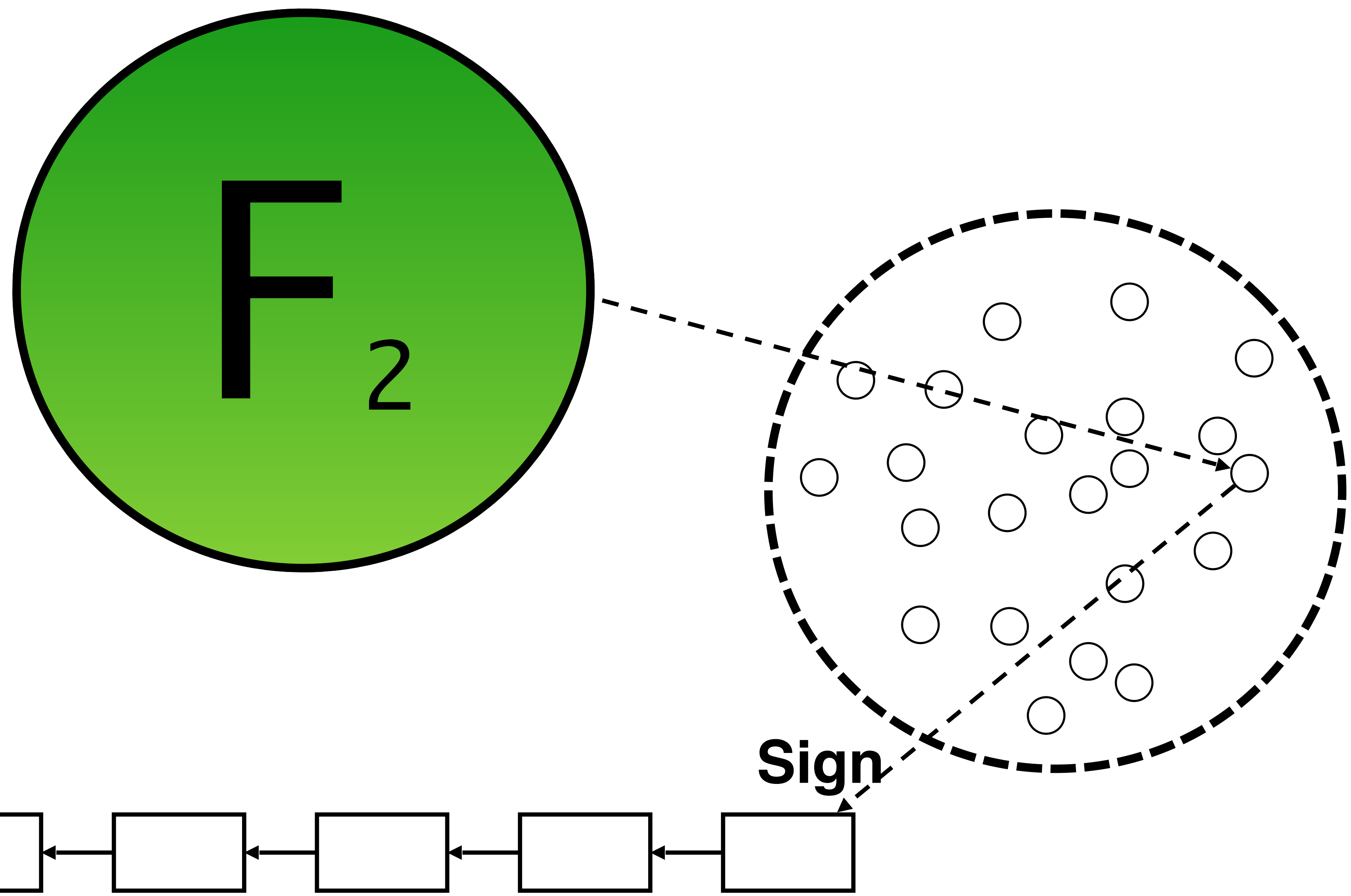

F

Beacon-based Blockchain

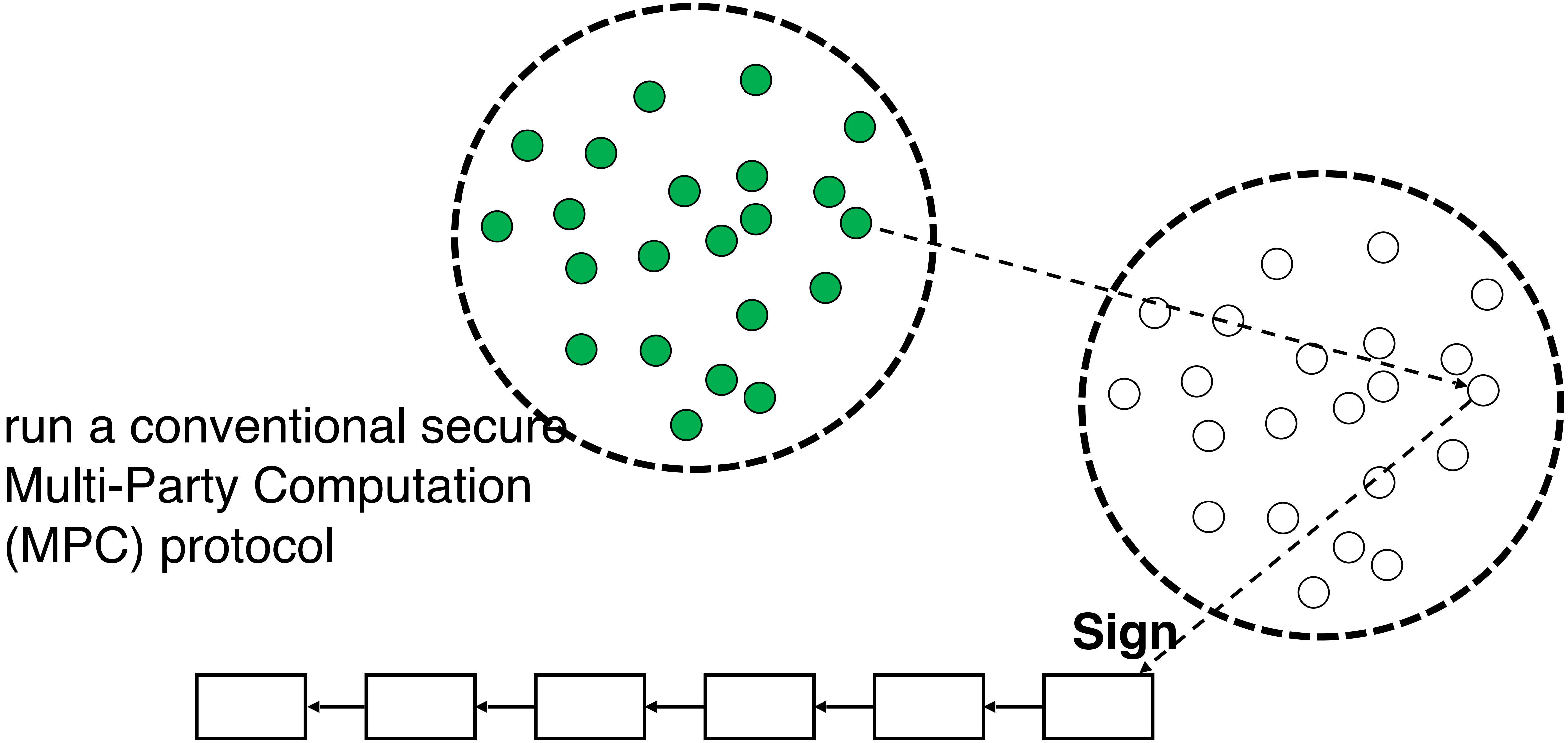


Beacon-based Blockchain

consider an *environment friendly* beacon functionality

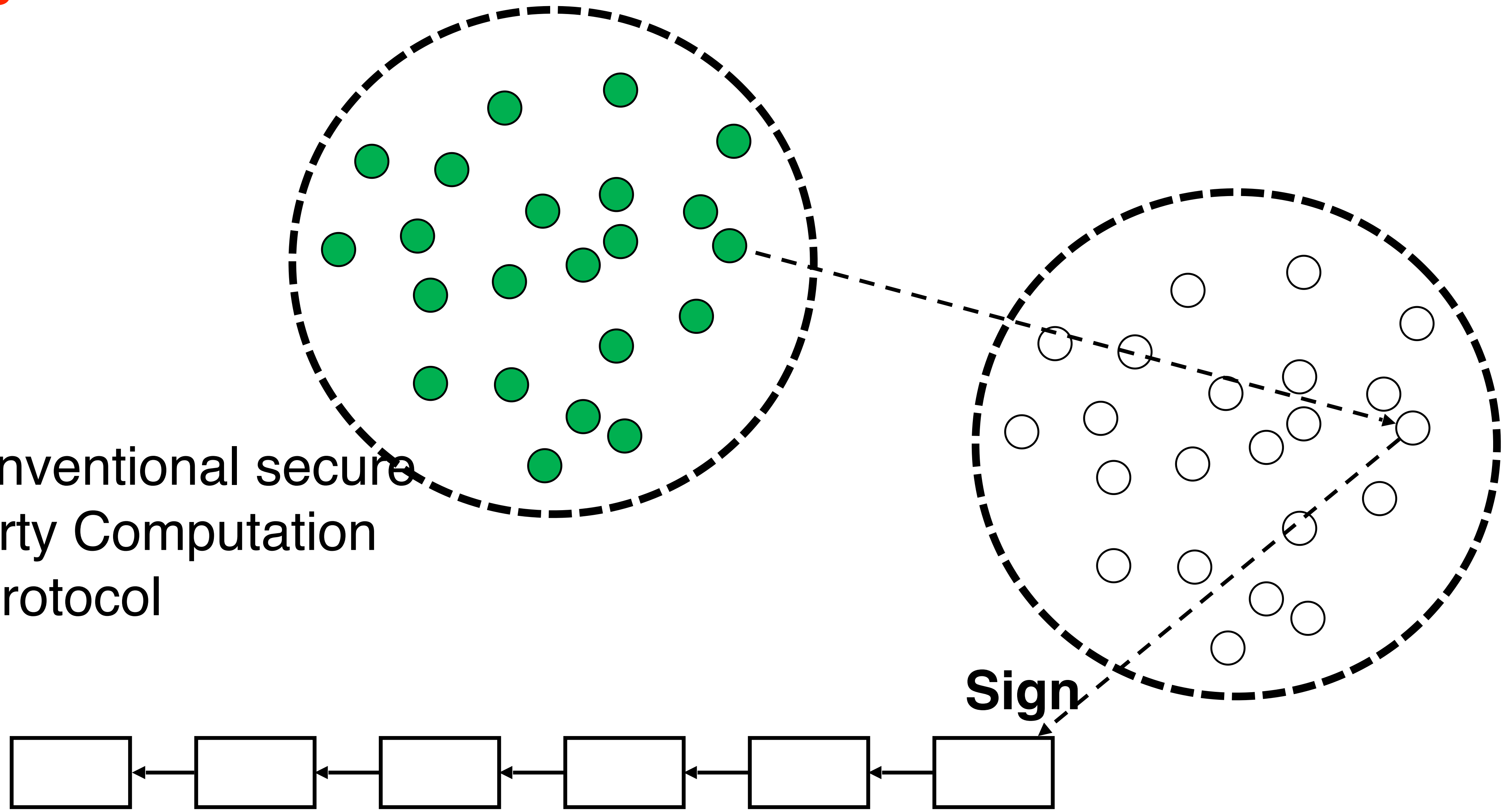


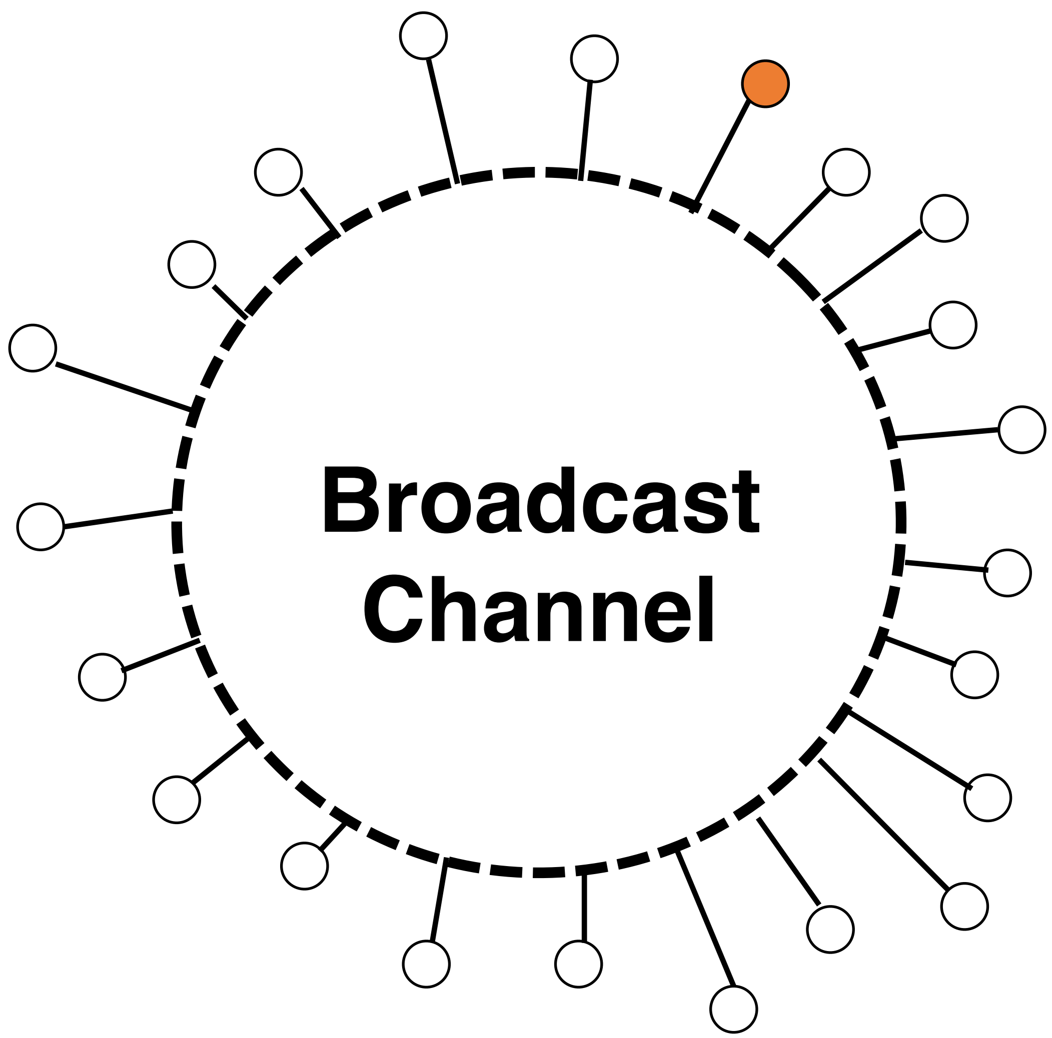
Conventional MPC-based Blockchain

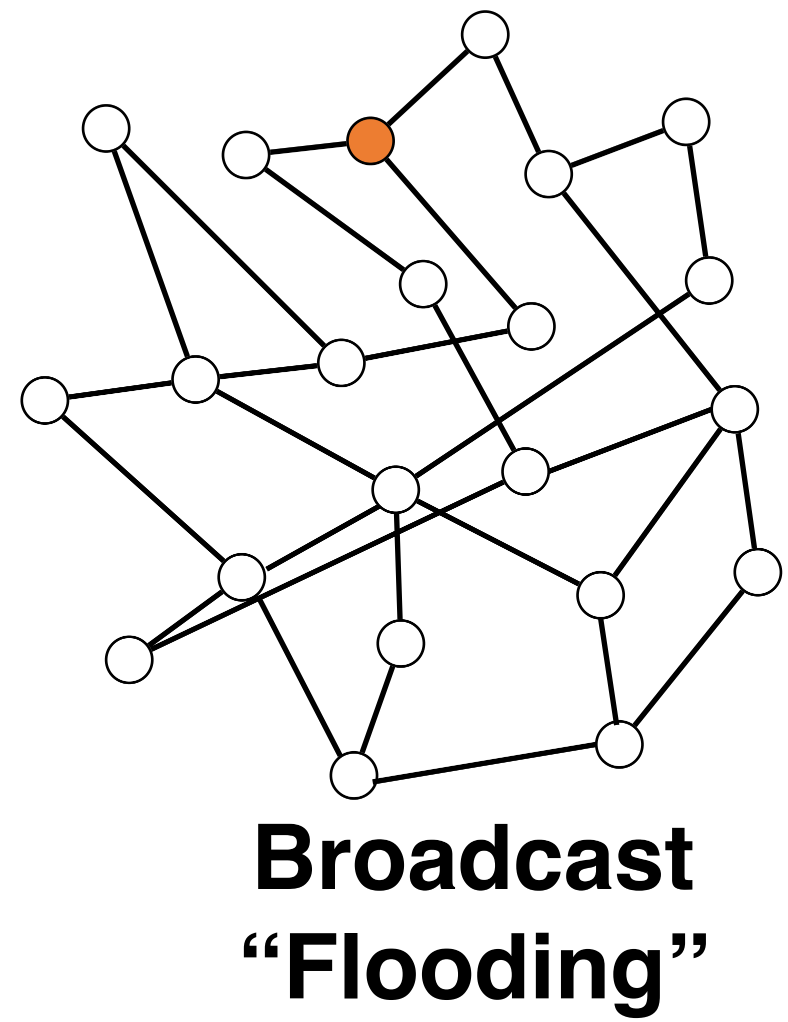


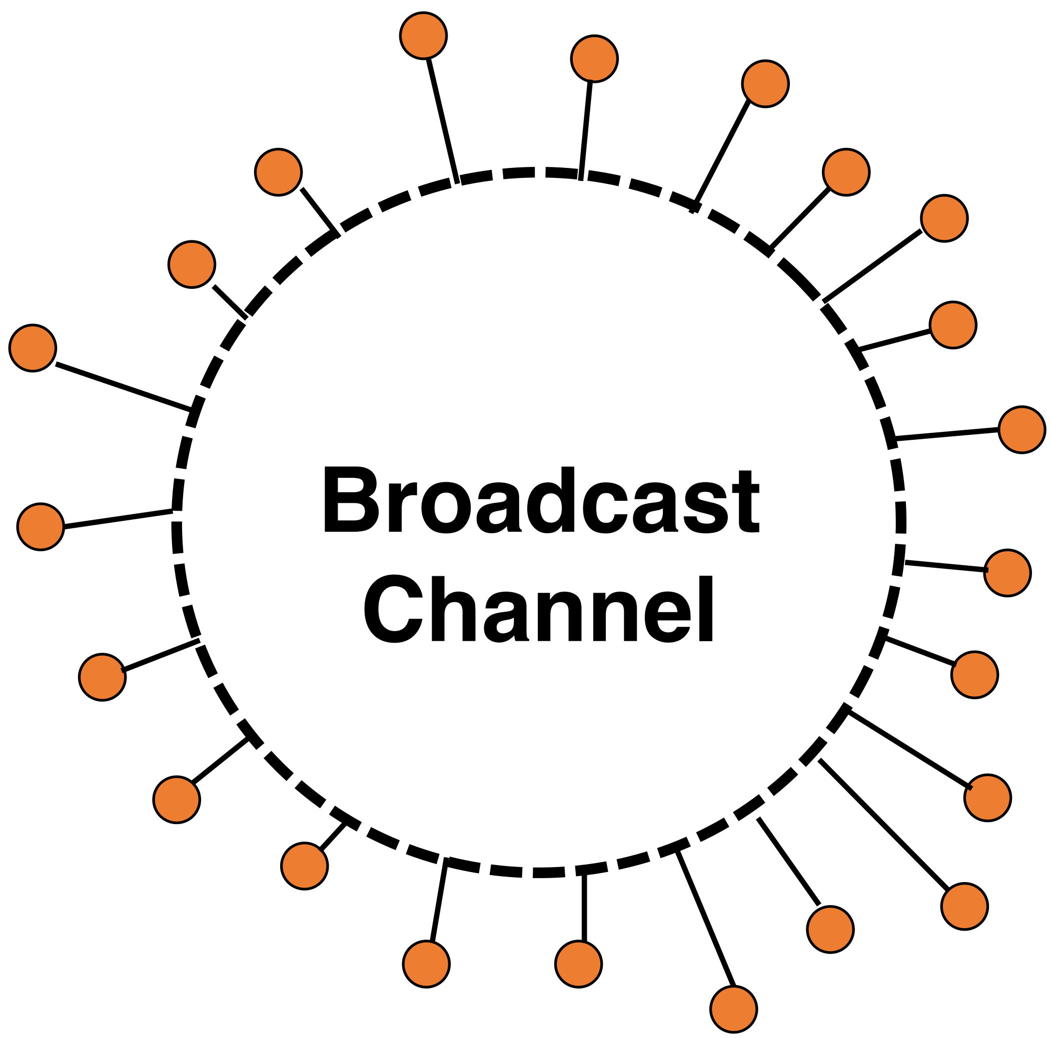
our goal is to obtain a large-scale blockchain.
Warning: Conventional MPC cannot scale.

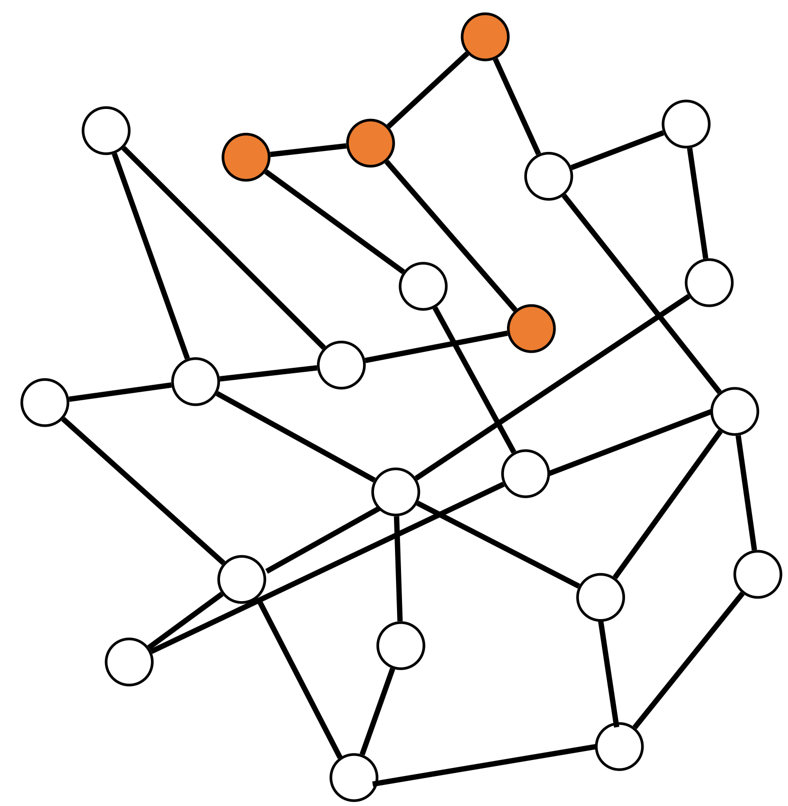
run a conventional secure Multi-Party Computation (MPC) protocol



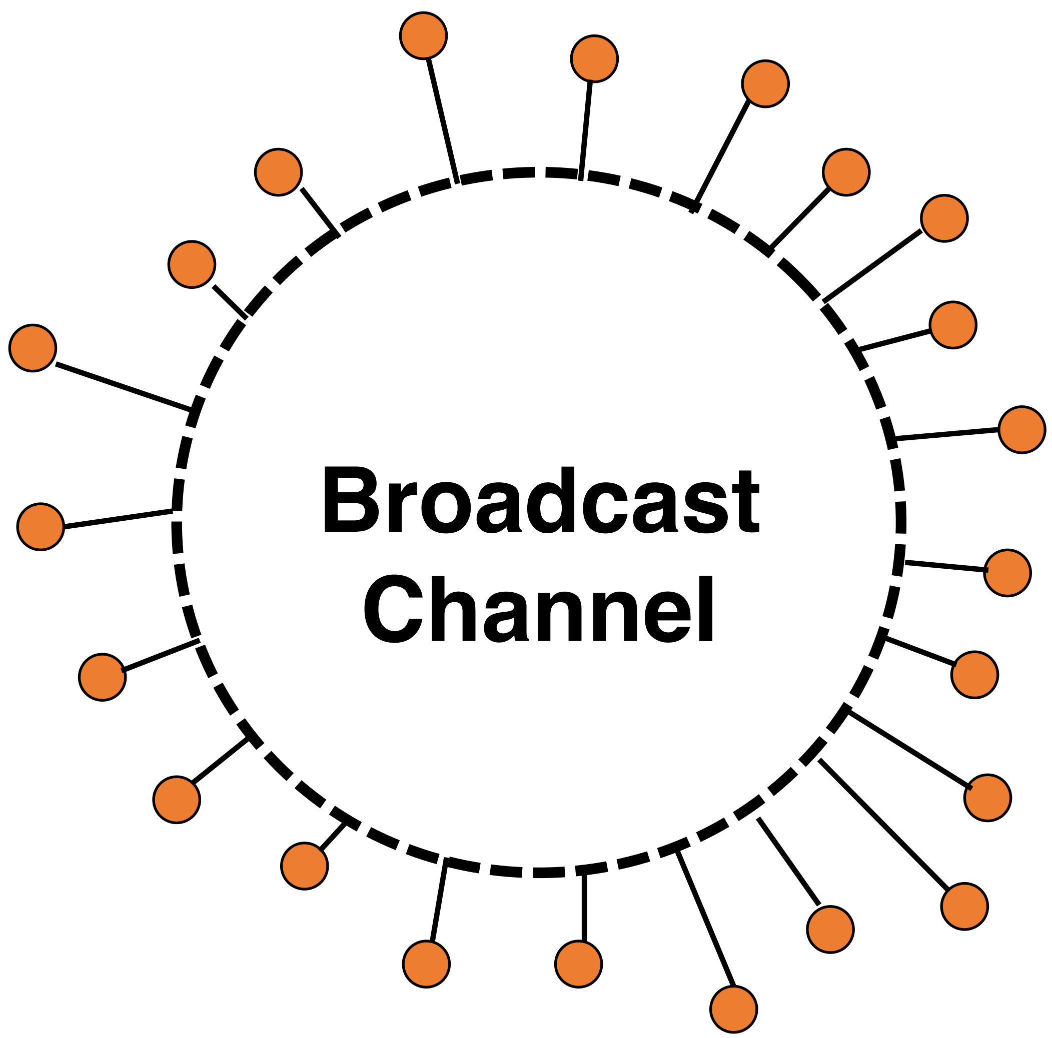

Broadcast
Channel

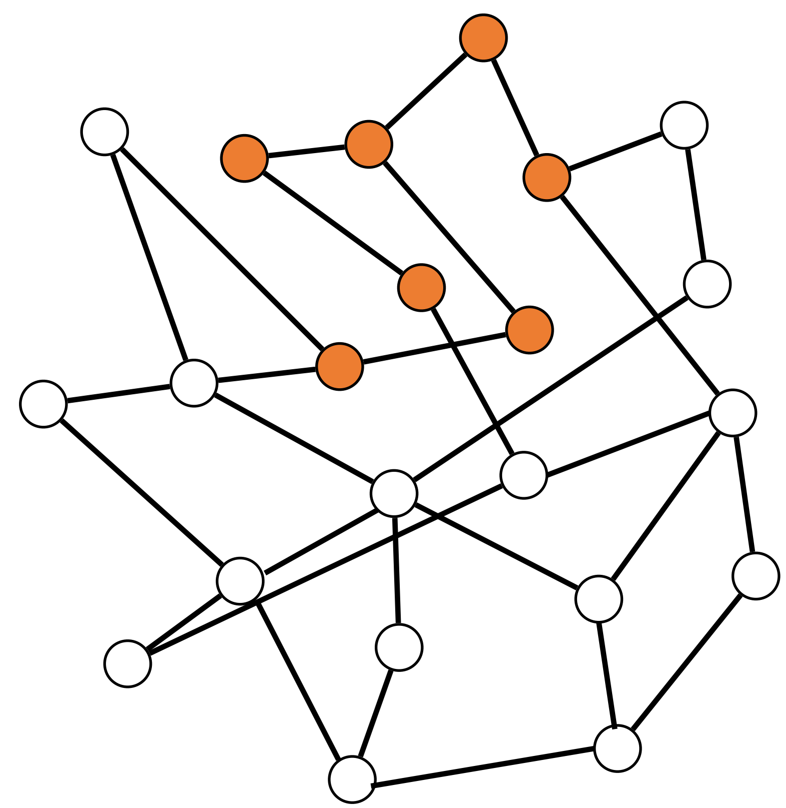

Broadcast
“Flooding”



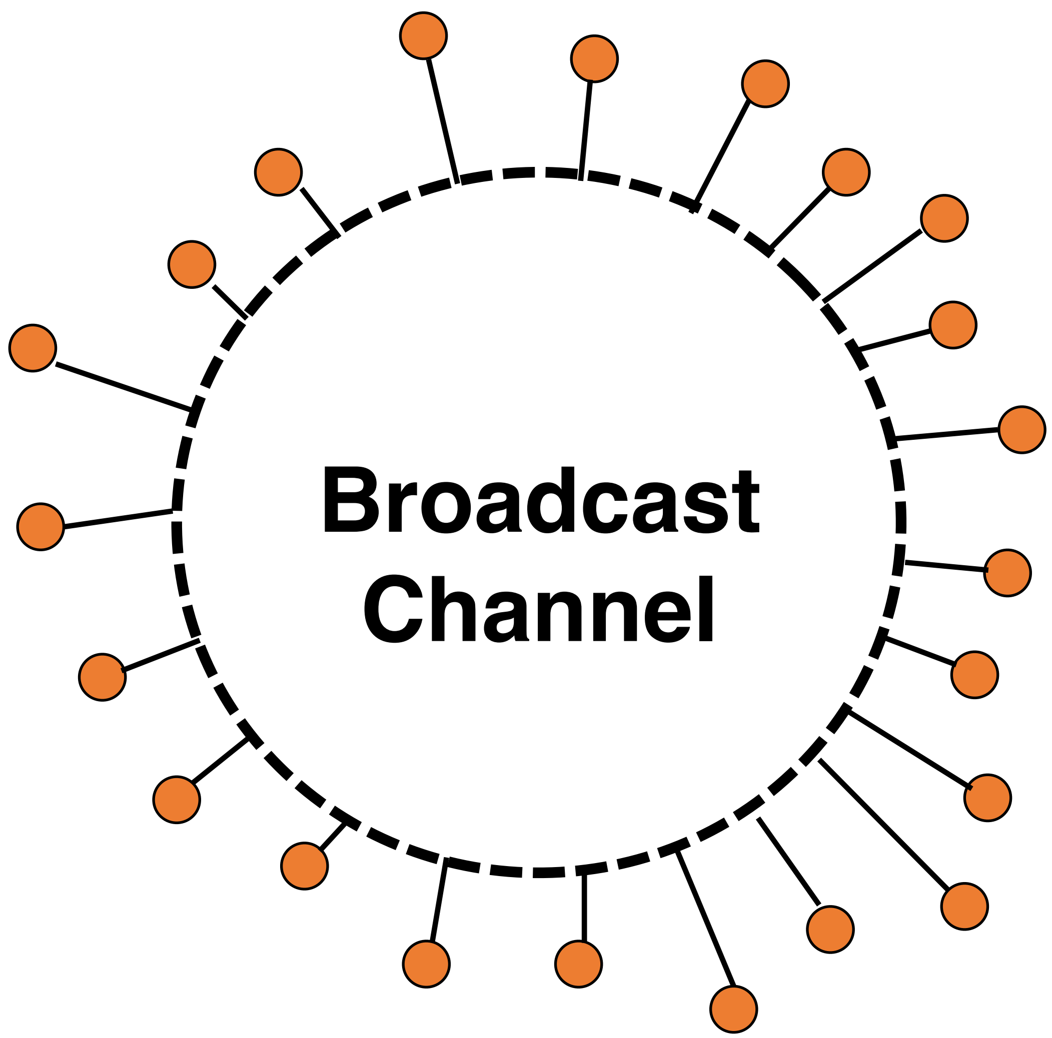


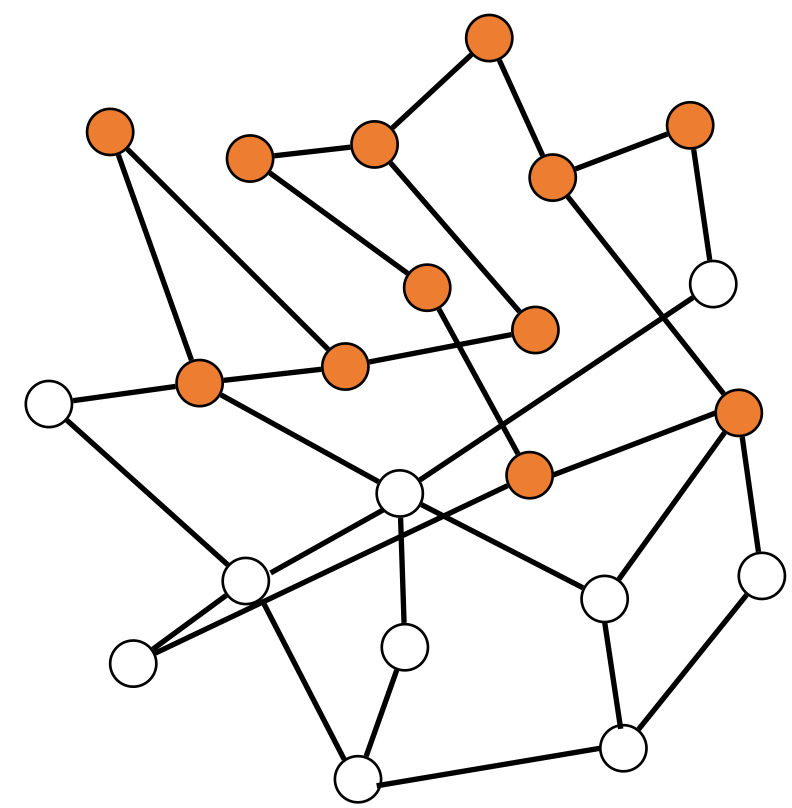
Broadcast
“Flooding”

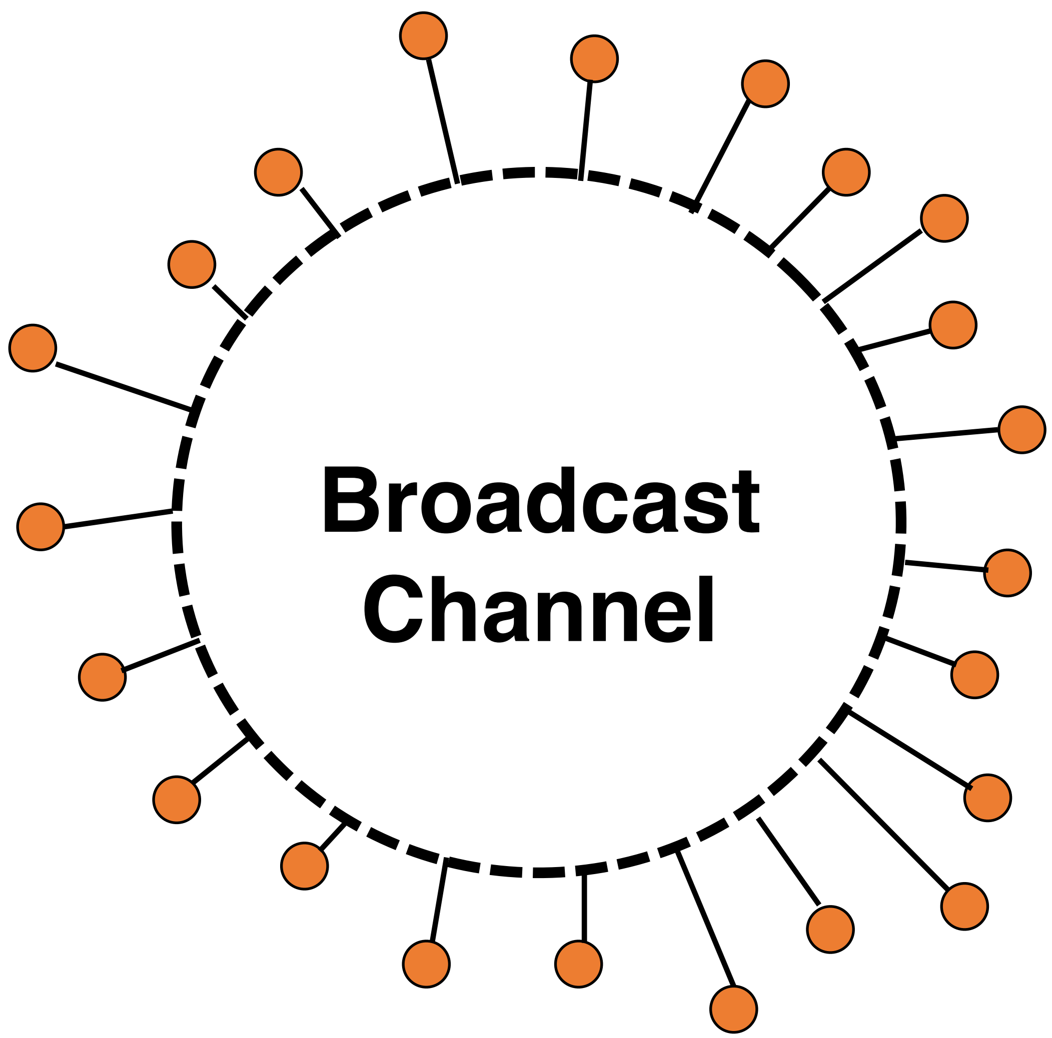


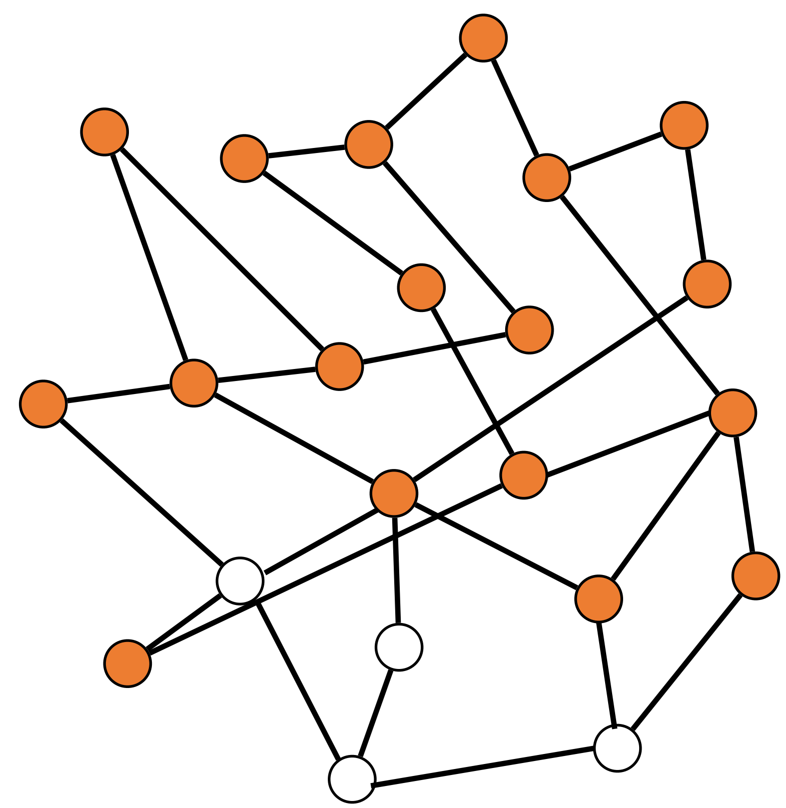


Broadcast
“Flooding”

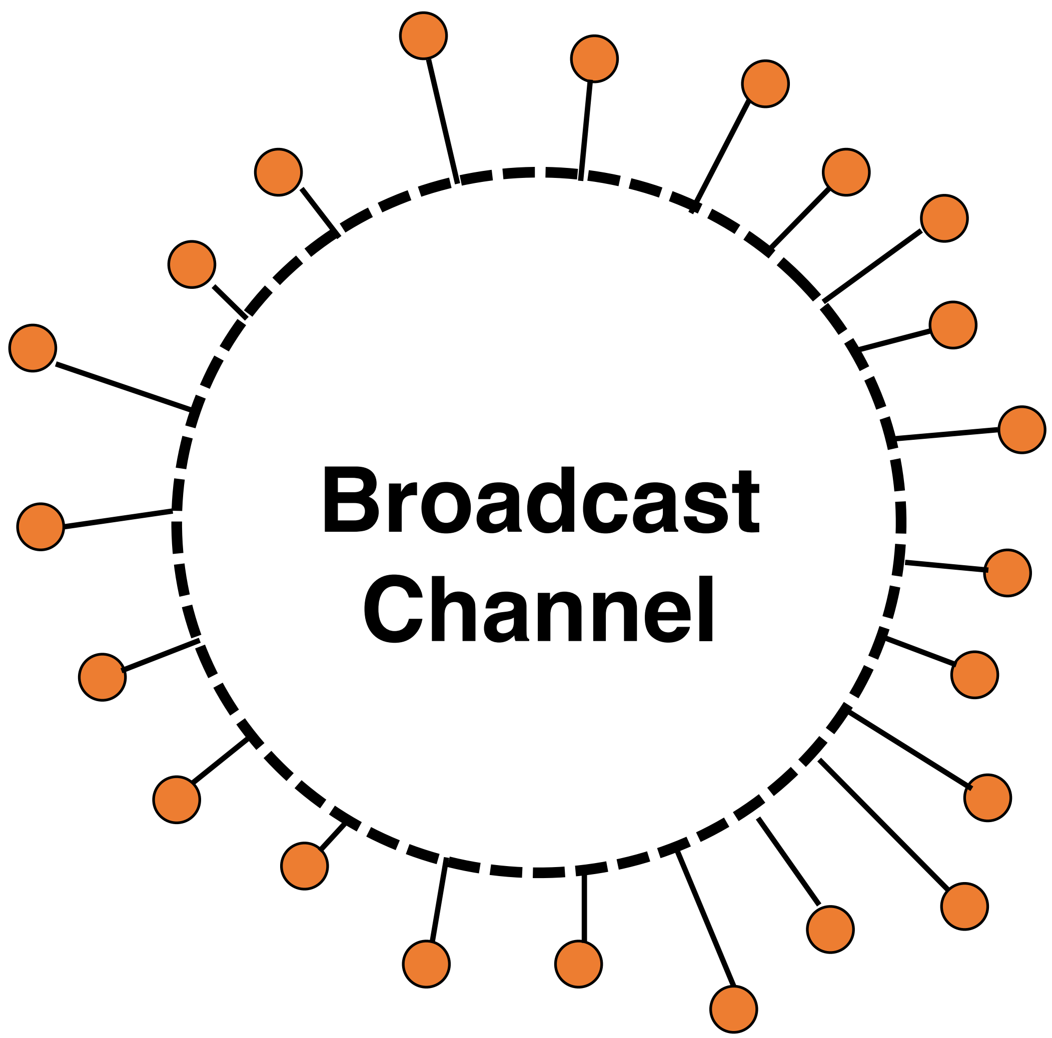

Broadcast
Channel

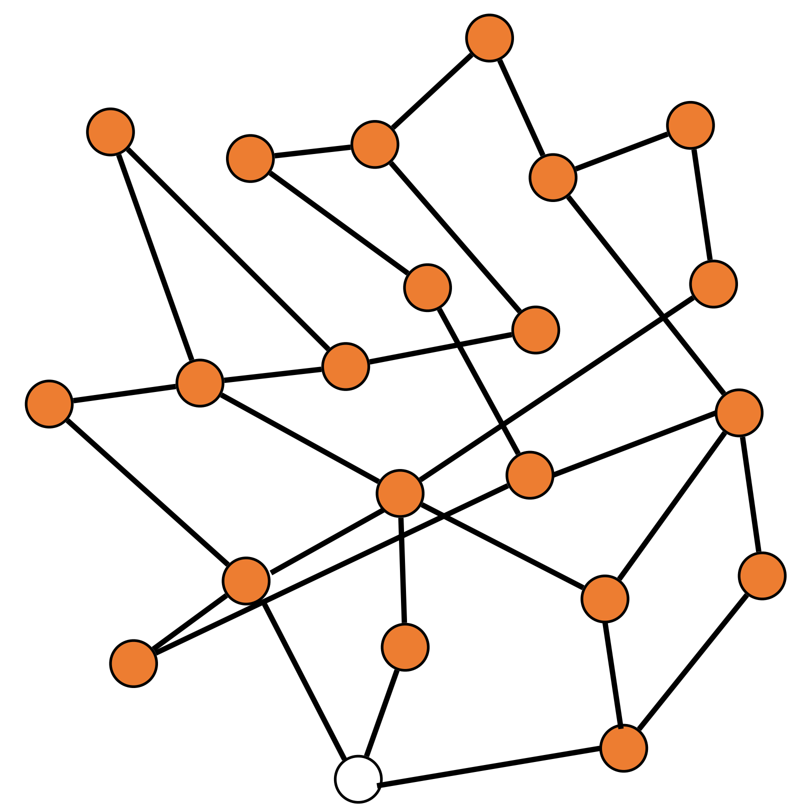

Broadcast
“Flooding”



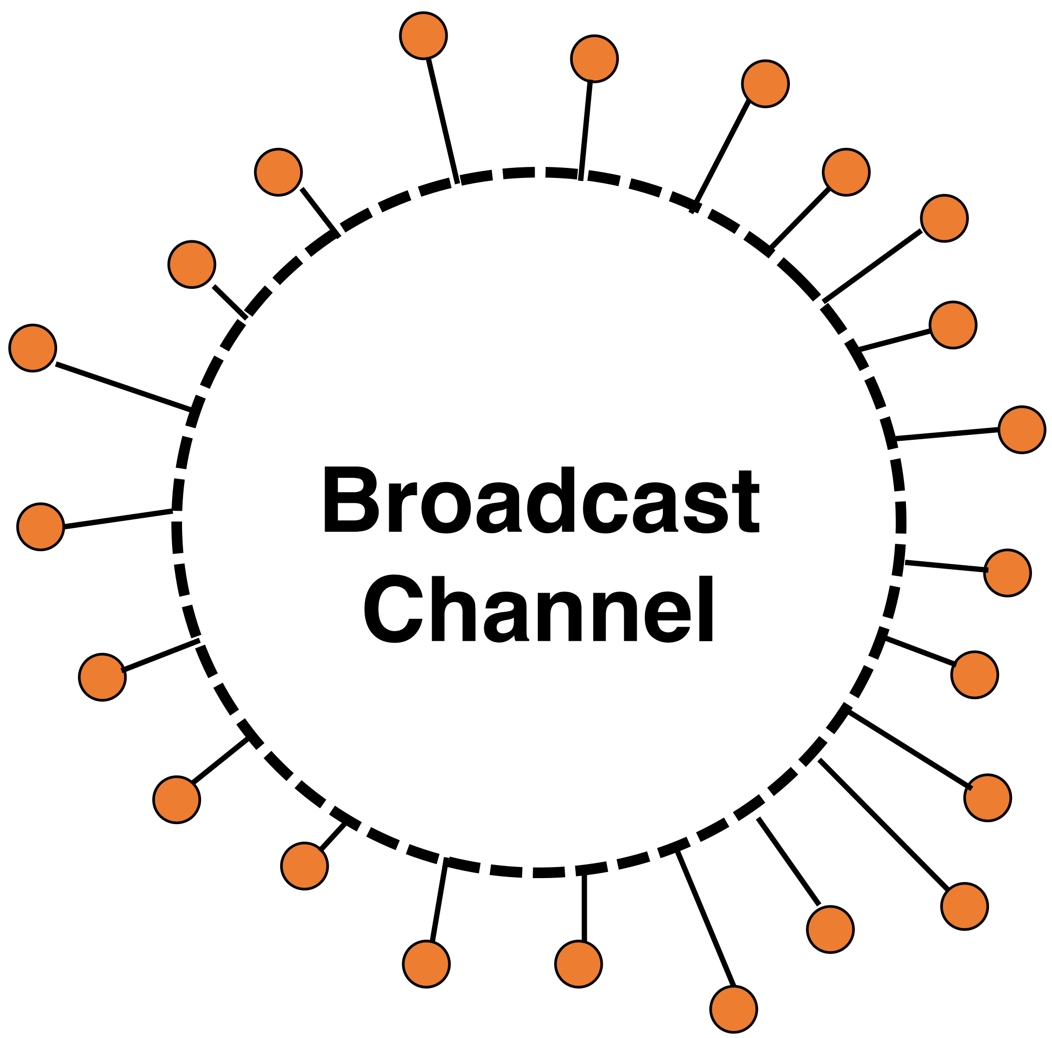


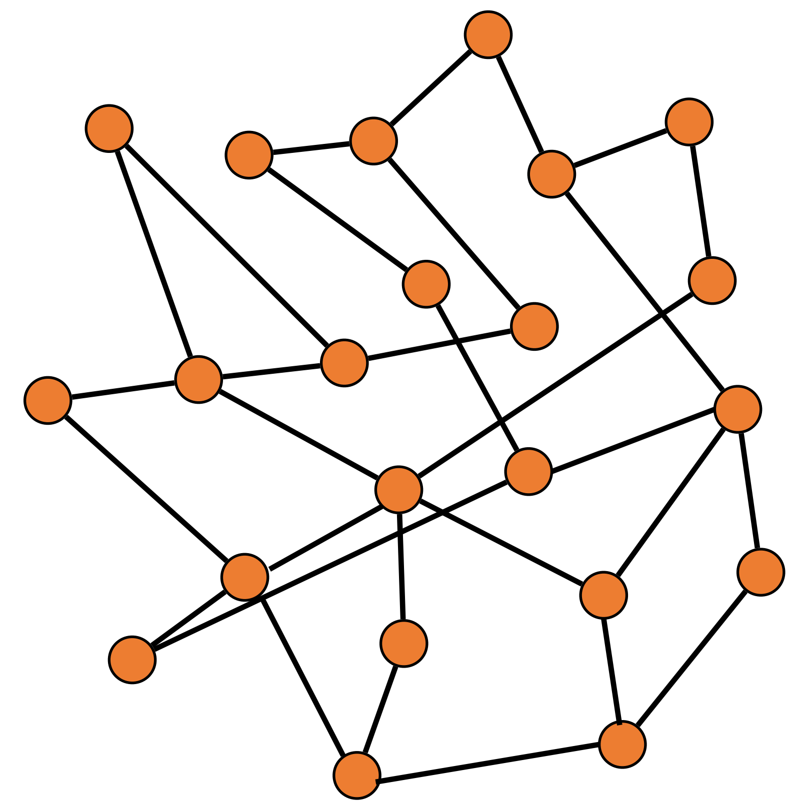
Broadcast
“Flooding”





Broadcast
“Flooding”





Broadcast
“Flooding”

Communication Complexity for 1 Message is $\Theta(n)$.

Lightweight communication protocols:

- constant ***c*** messages are broadcast;
- communication complexity is $\Theta(n)$.
- can scale to a huge network

Heavy communication protocols:

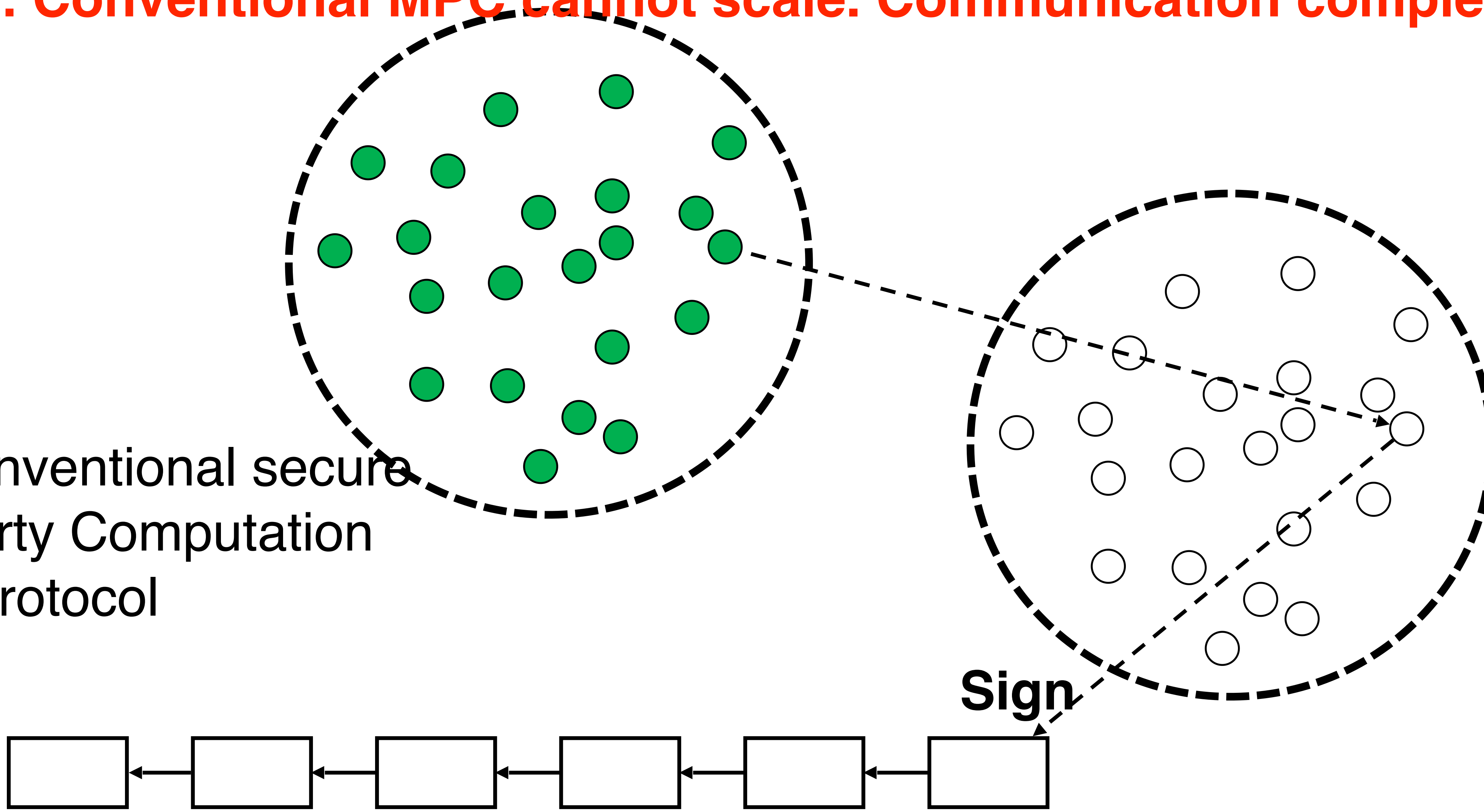
- such as voting needs;
- $\Theta(n)$ messages are broadcast;
- communication complexity is $\Theta(n^2)$.
- It is not scalable.

Conventional MPC-based Blockchain

our goal is to obtain a large-scale blockchain.

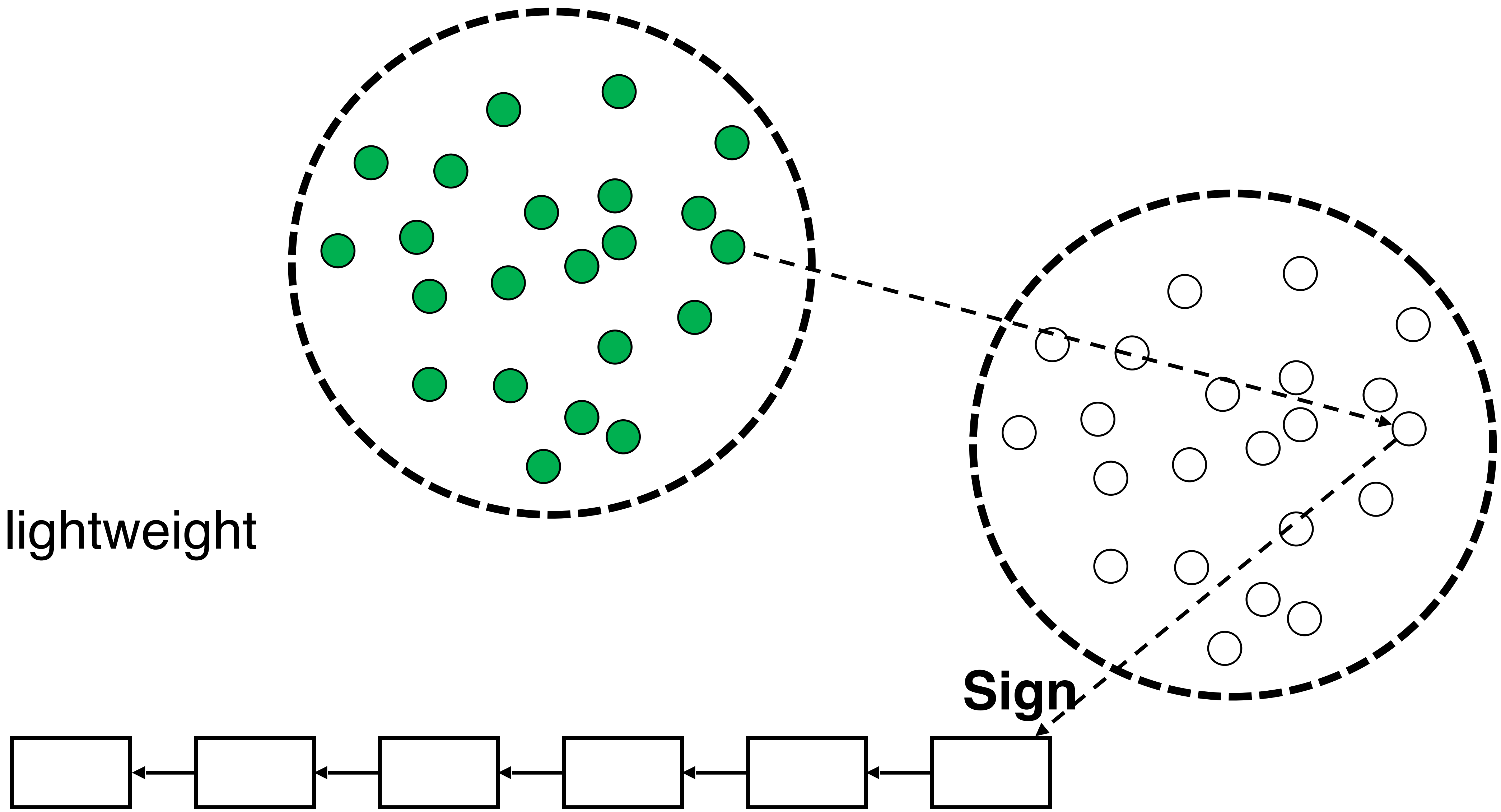
Warning: Conventional MPC cannot scale. Communication complexity (n^2)

run a conventional secure Multi-Party Computation (MPC) protocol

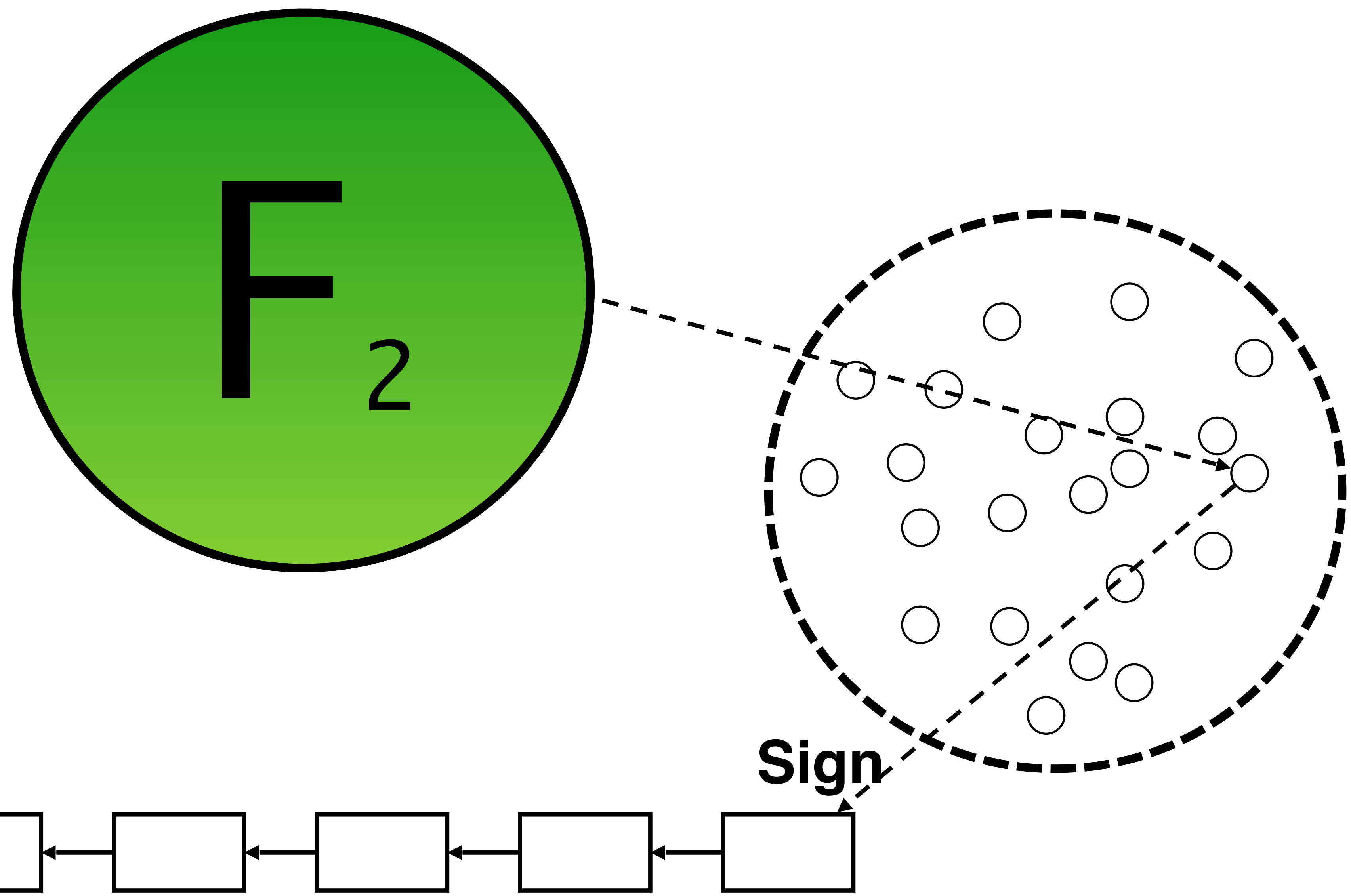


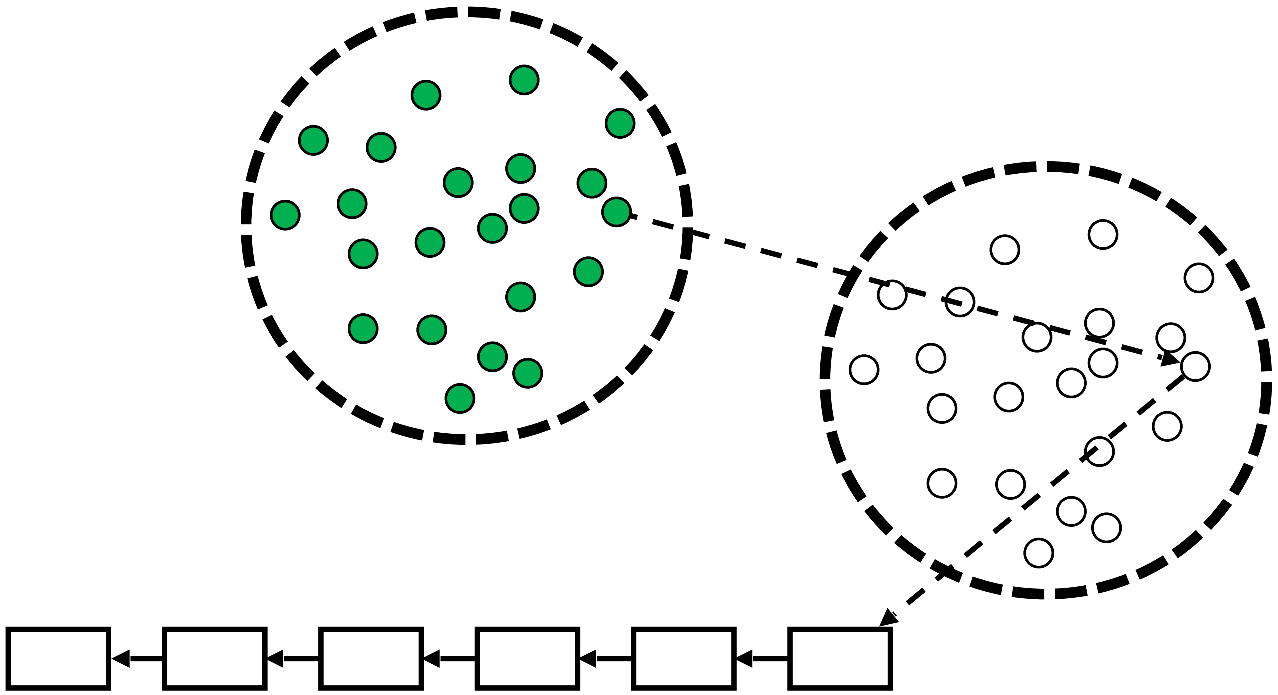
only lightweight blockchains scale

expect a lightweight
protocol

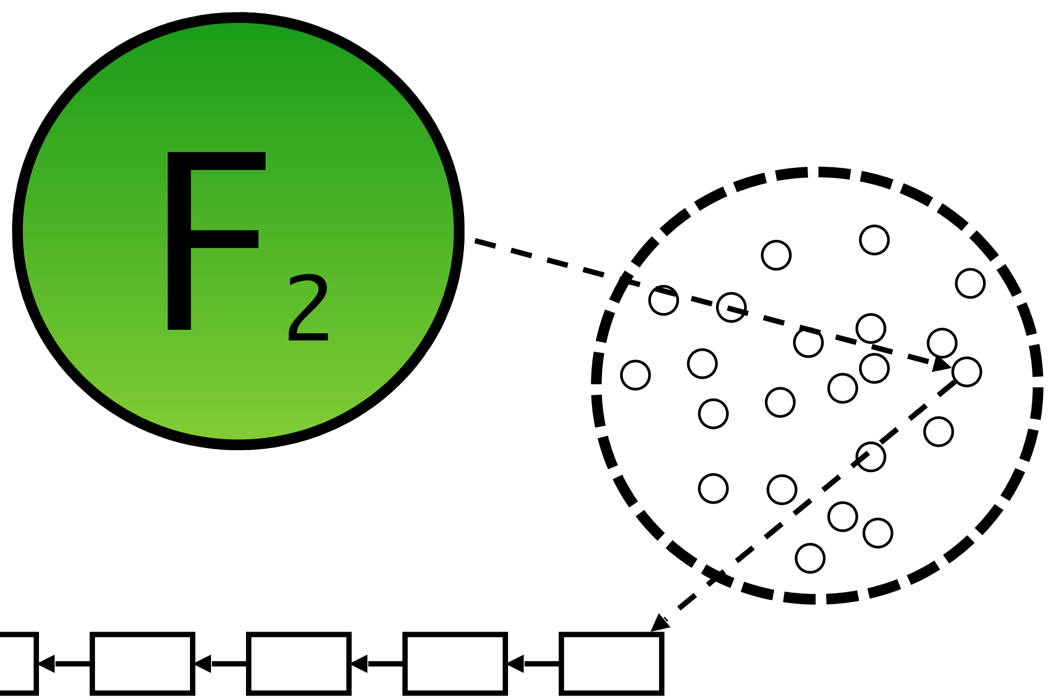


consider an *environment friendly* beacon functionality





if we can design a
lightweight protocol

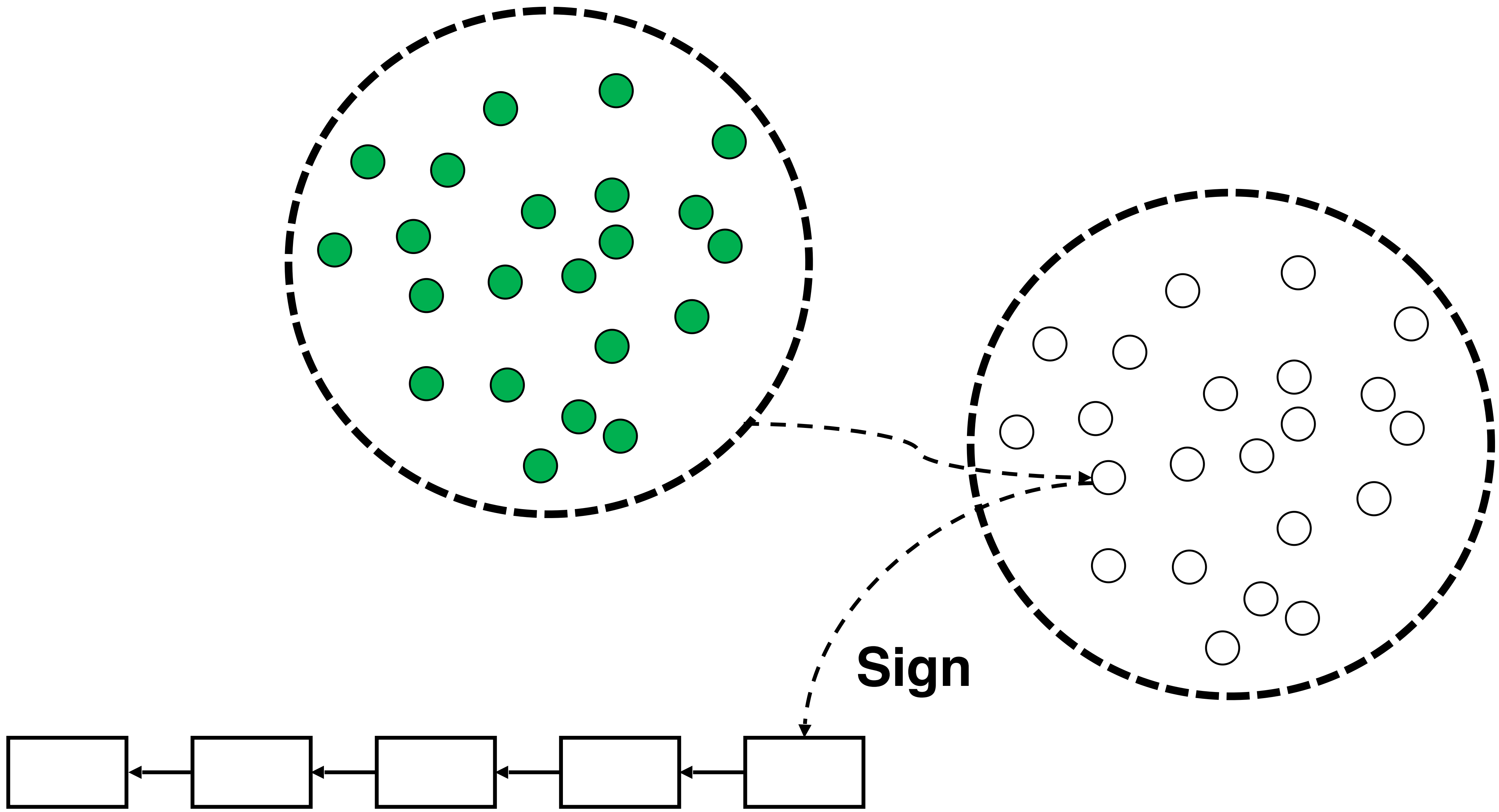


which achieves an
environment
friendly beacon
functionality

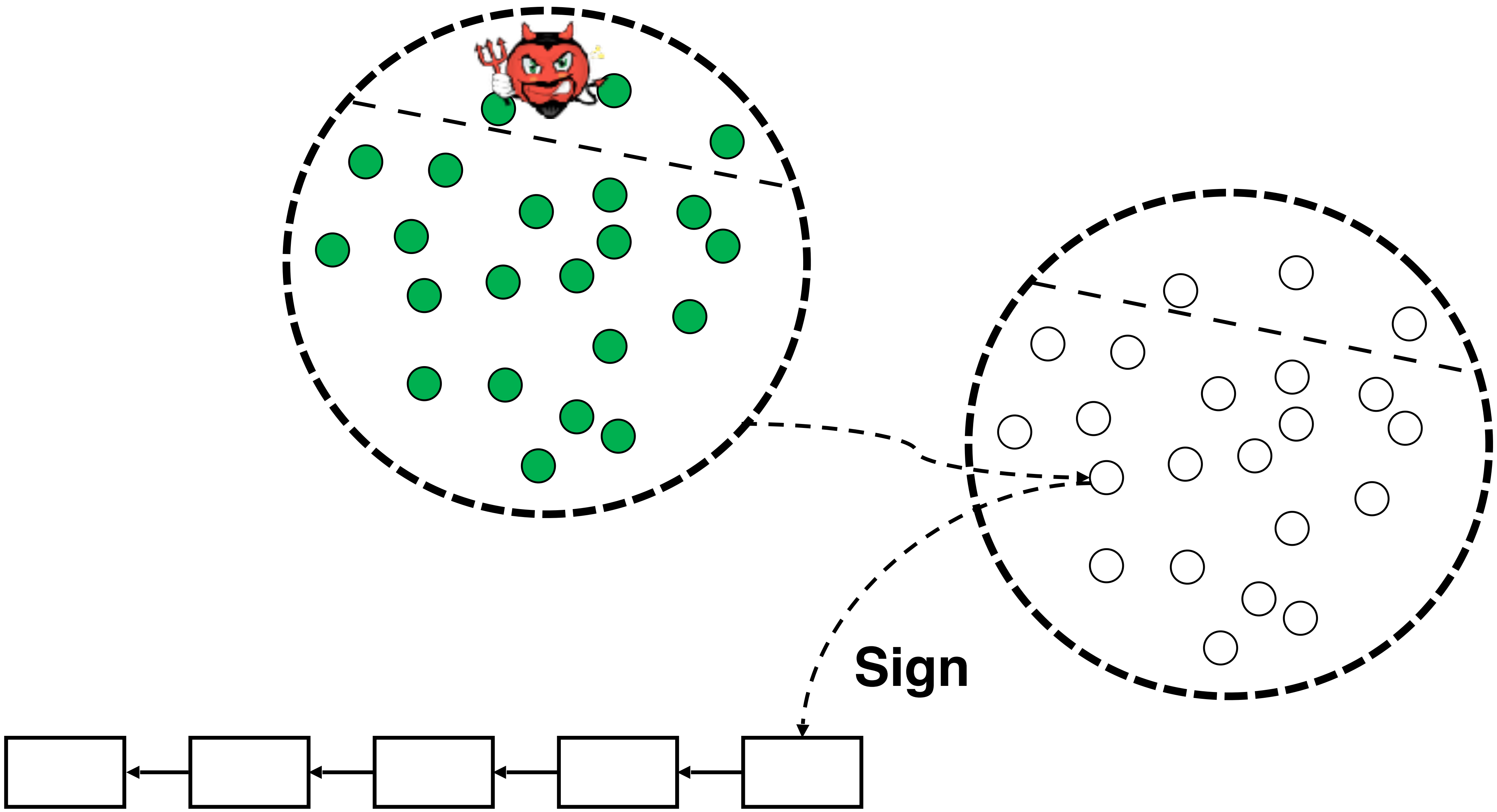
then we could make a
better blockchain than
Nakamoto's

However….main obstacle: splitting attack

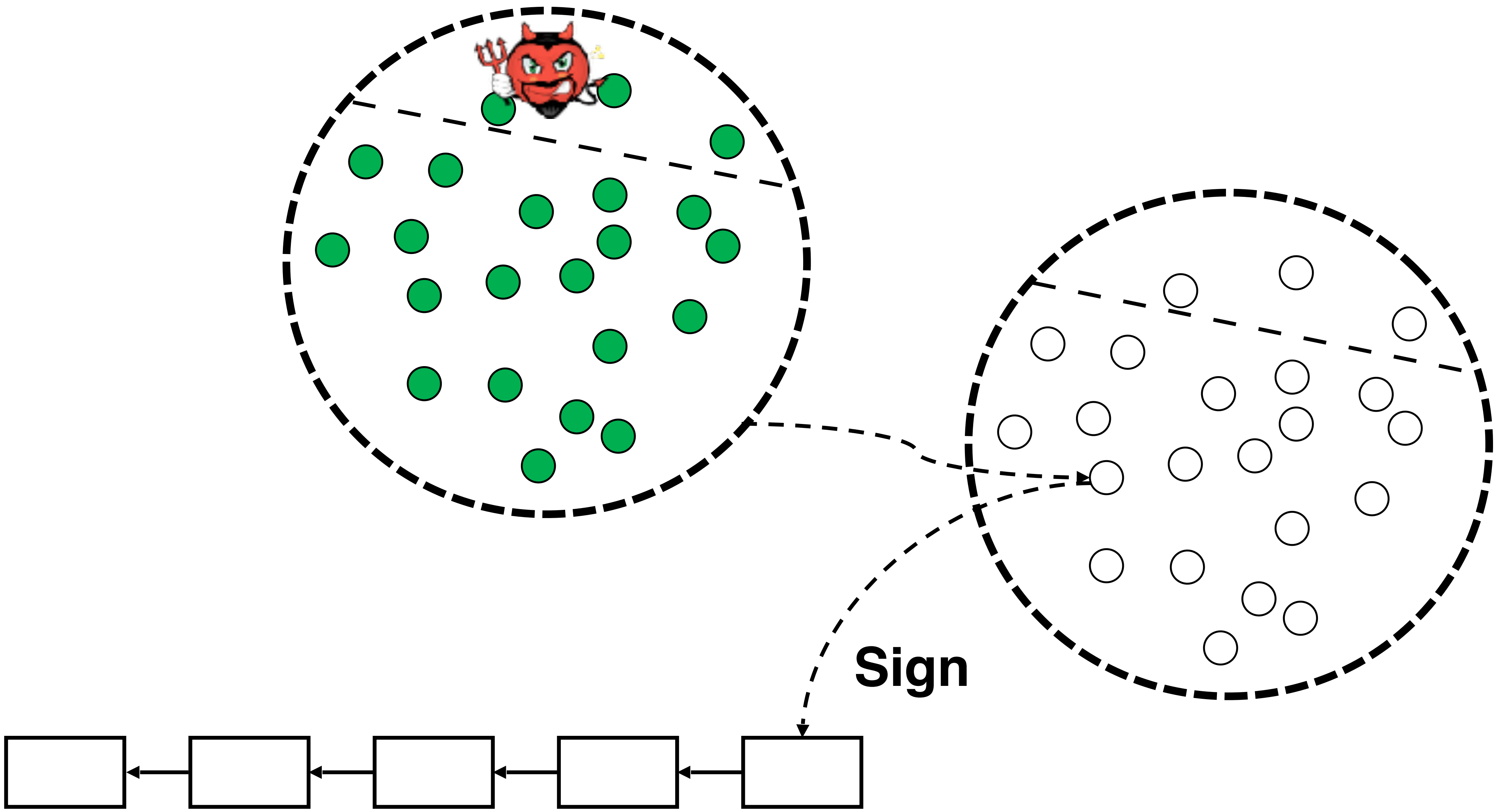
splitting attack on a class of lightweight protocols



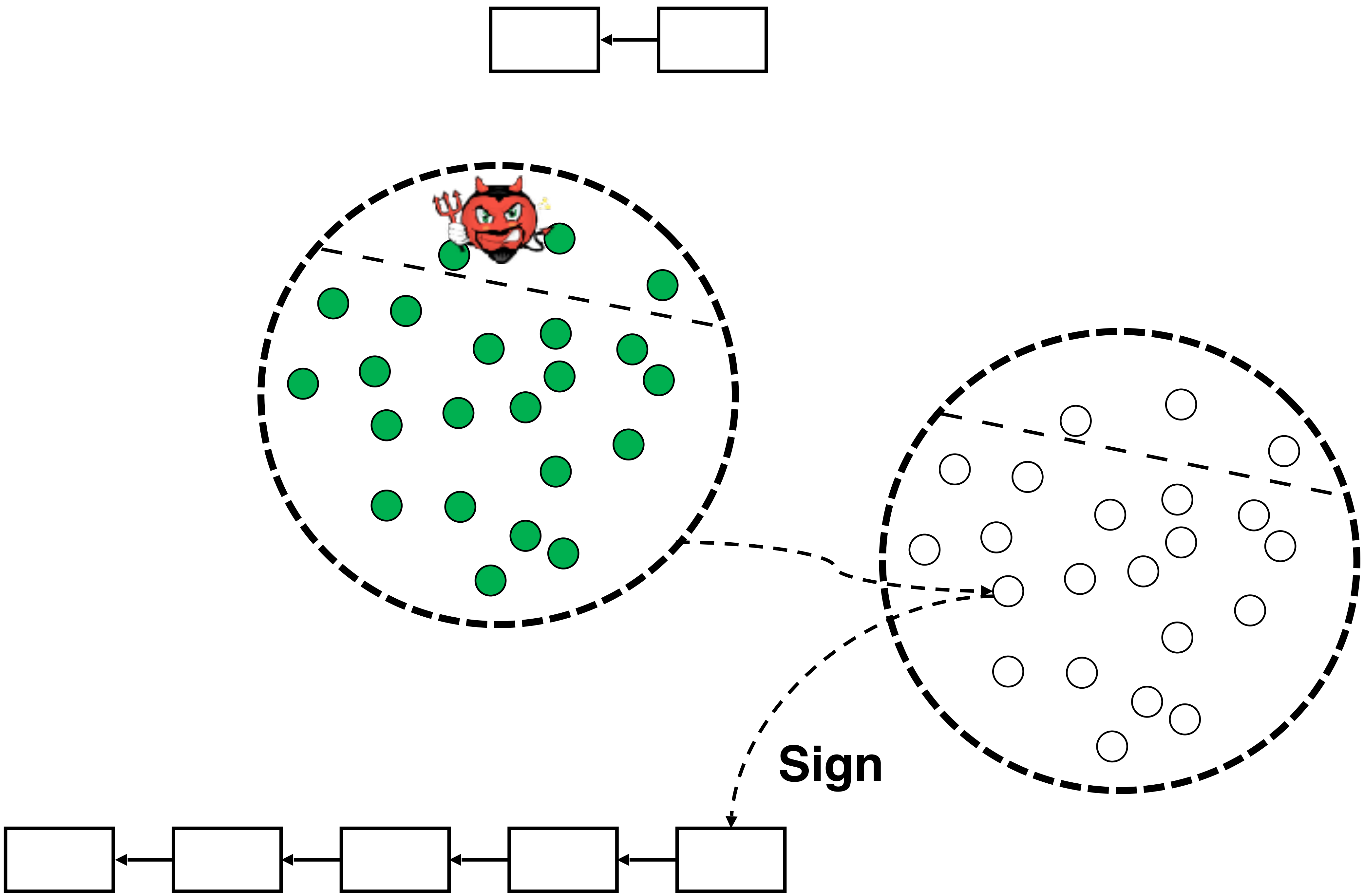
splitting attack on a class of lightweight protocols



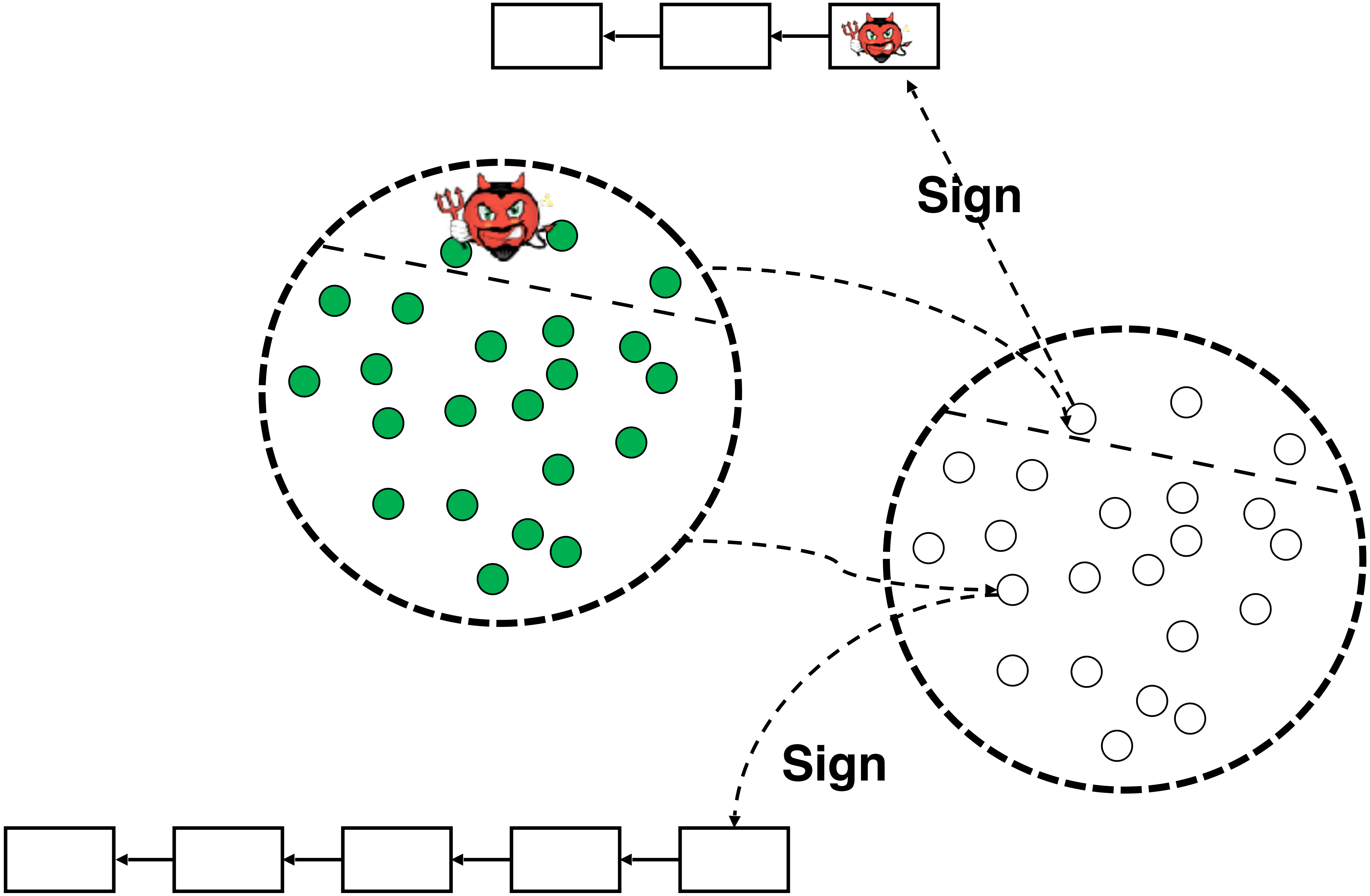
splitting attack on a class of lightweight protocols



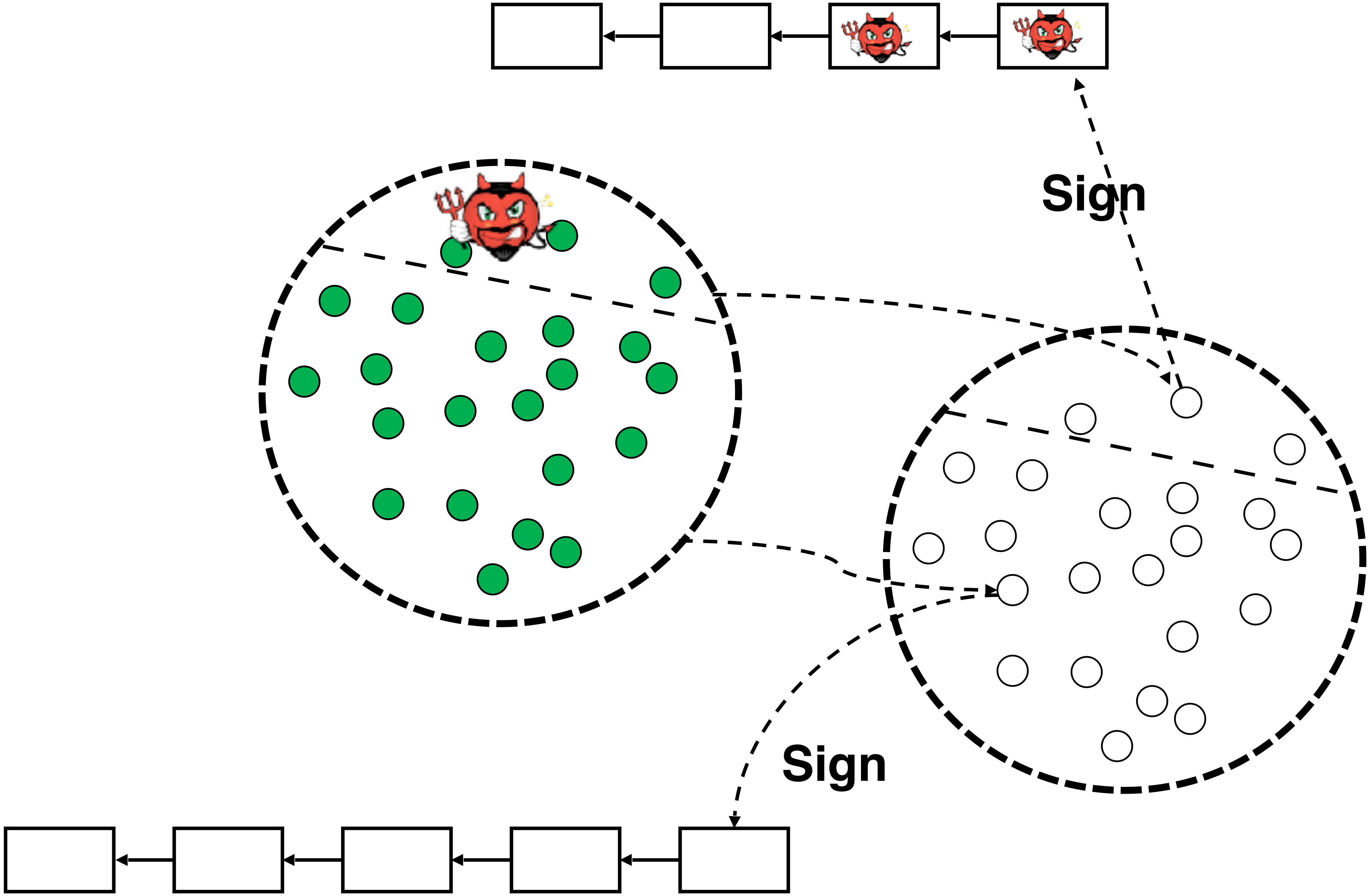
splitting attack on a class of lightweight protocols



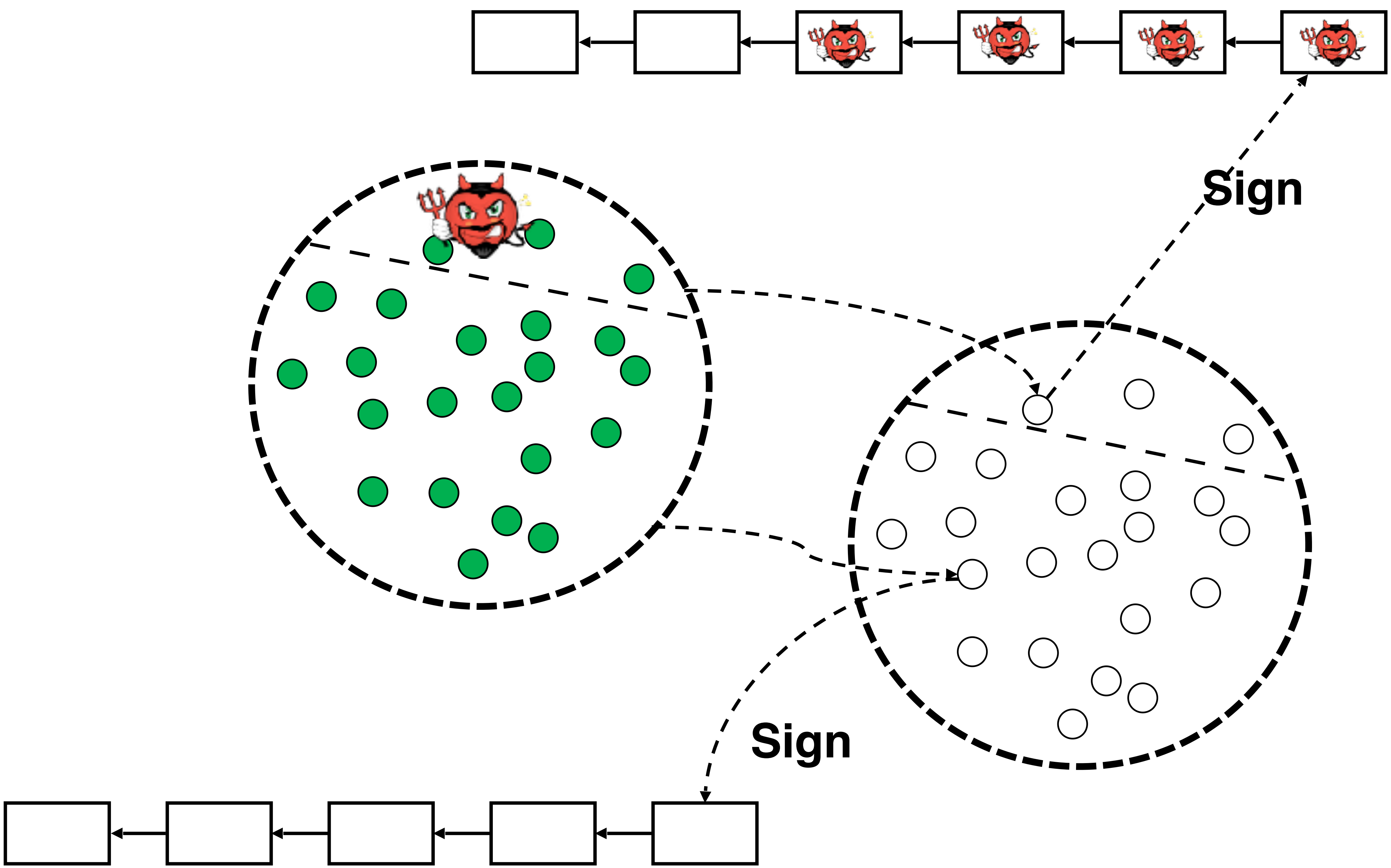
splitting attack on a class of lightweight protocols



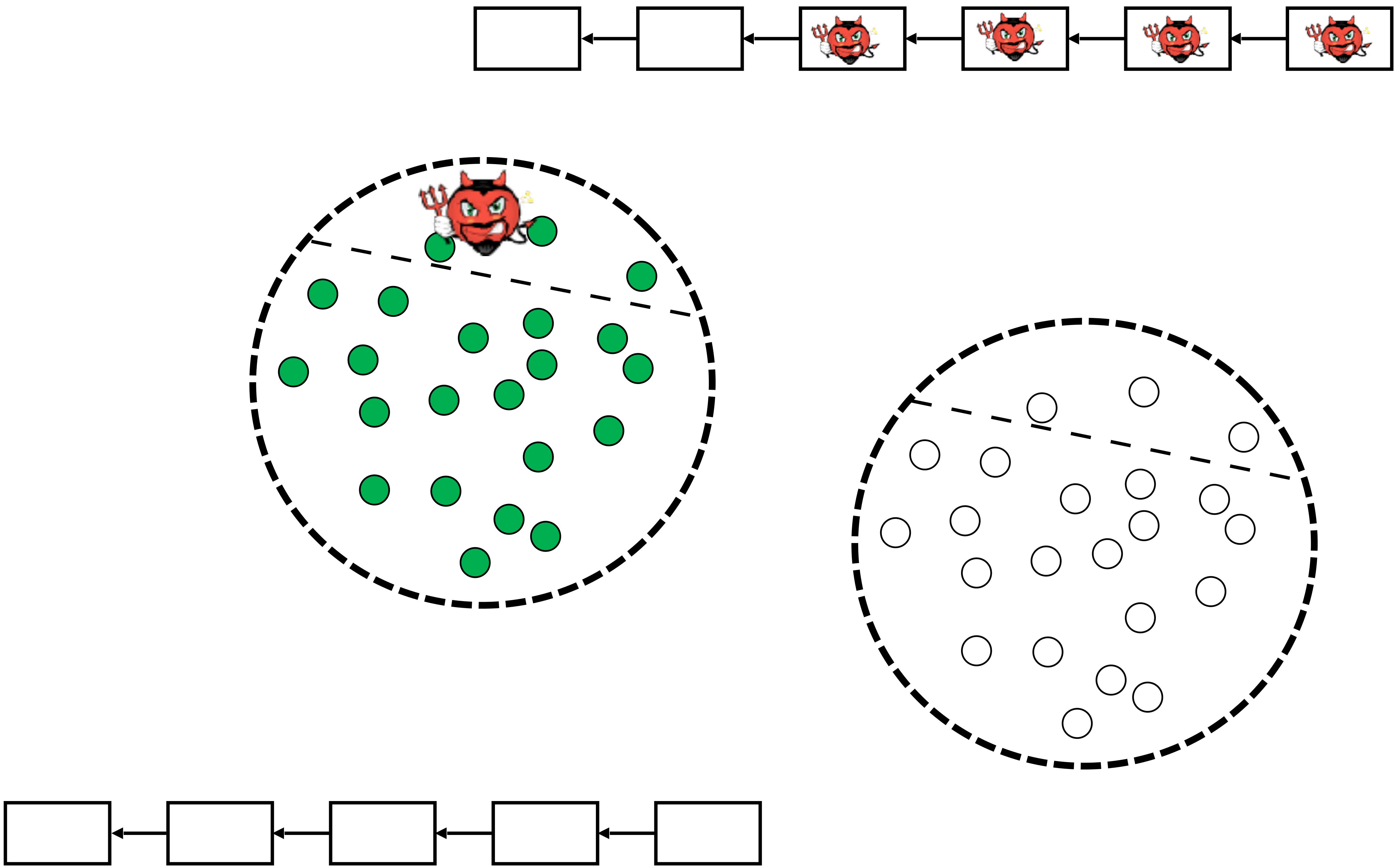
splitting attack on a class of lightweight protocols



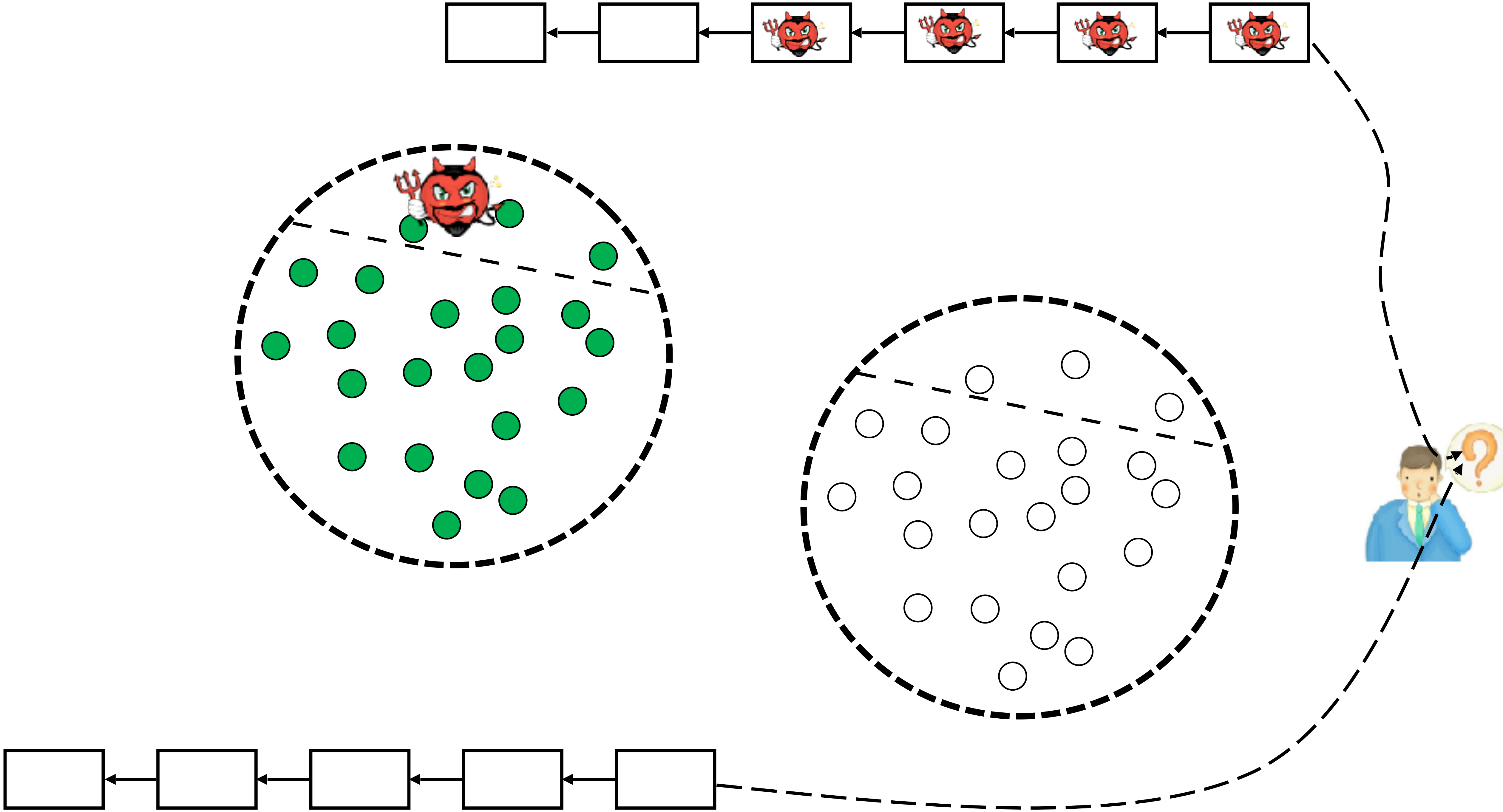
splitting attack on a class of lightweight protocols



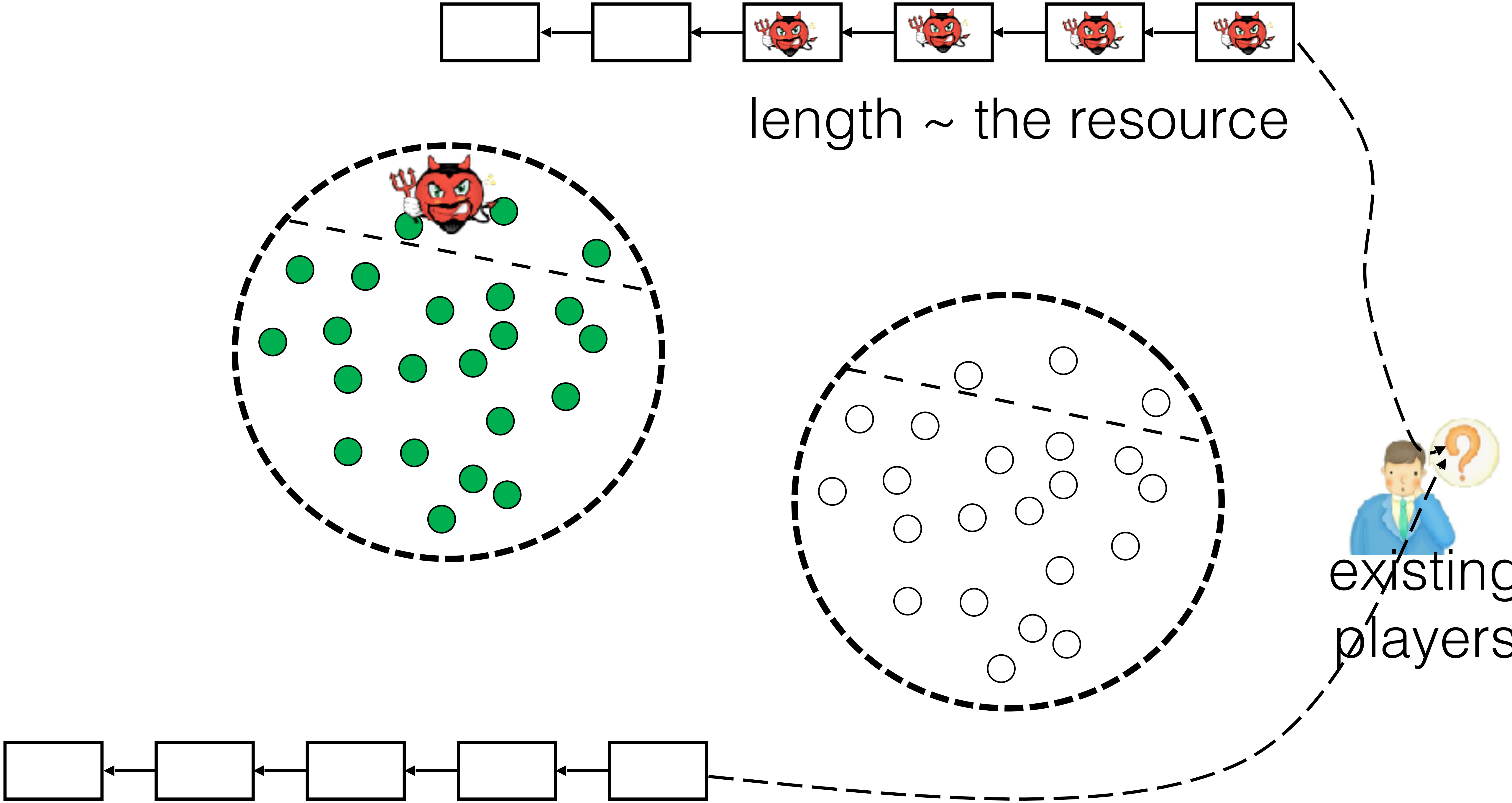
splitting attack on a class of lightweight protocols



splitting attack on a class of lightweight protocols

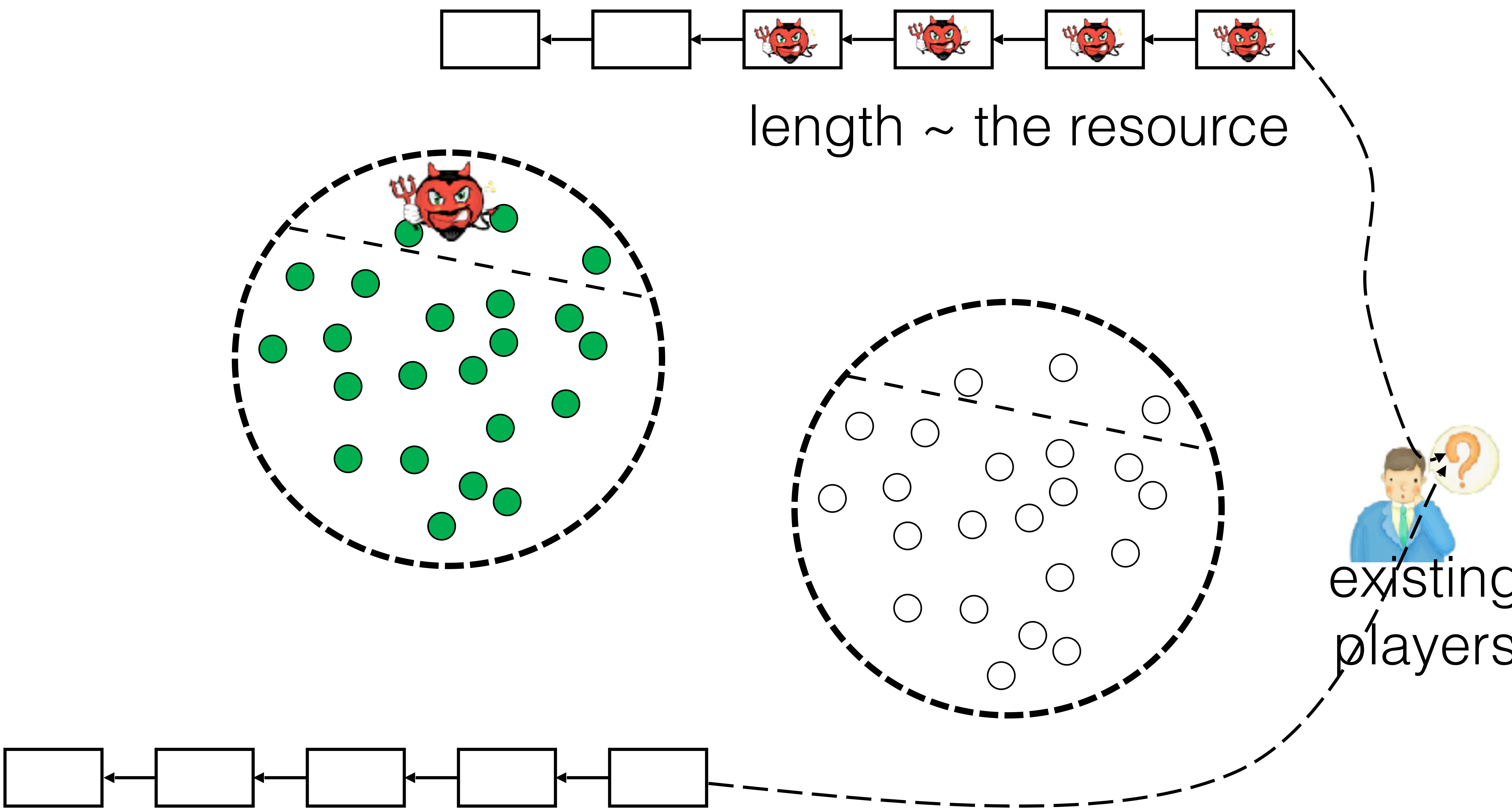


splitting attack on a class of lightweight protocols

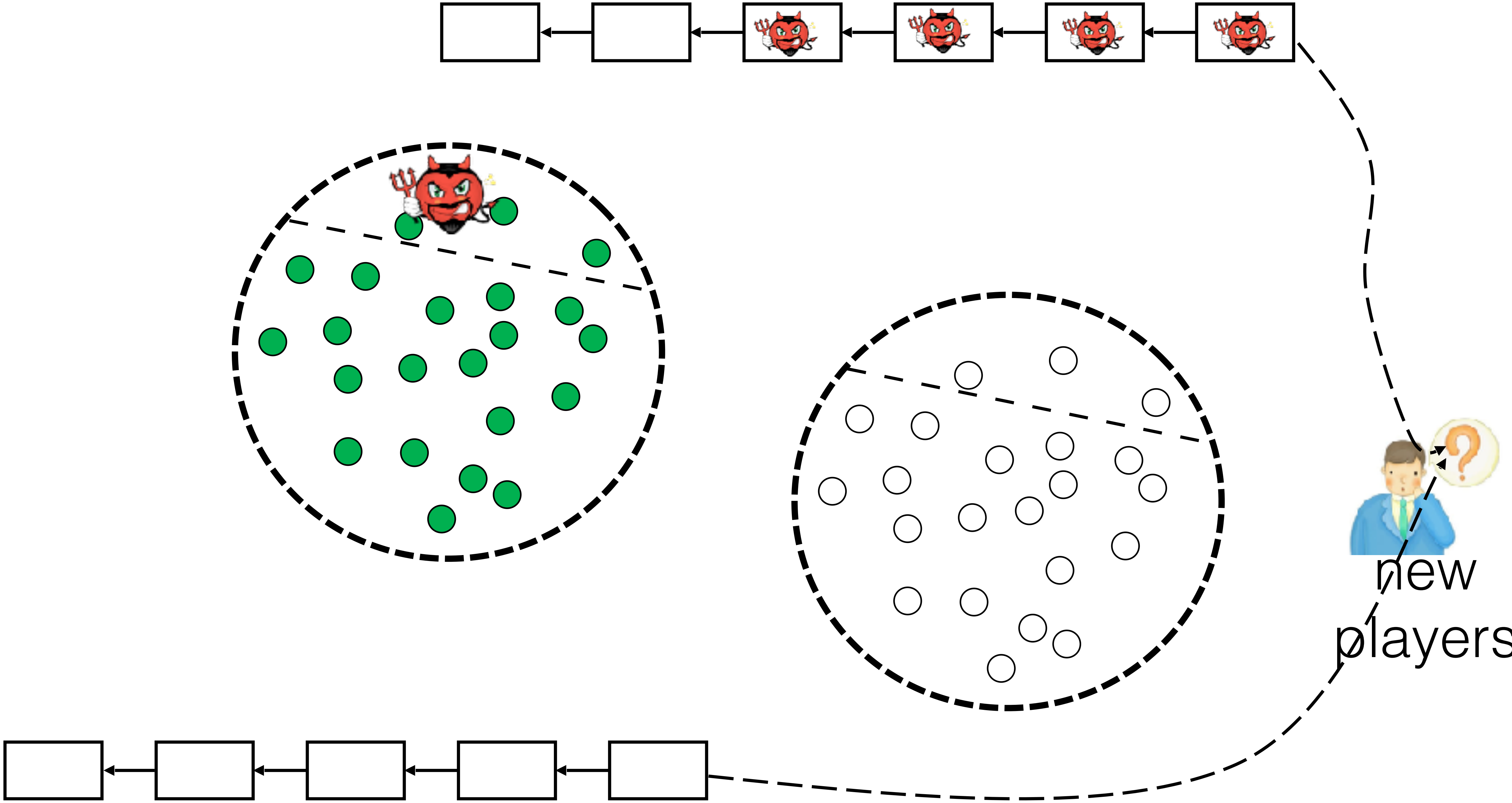


splitting attack on a class of lightweight protocols

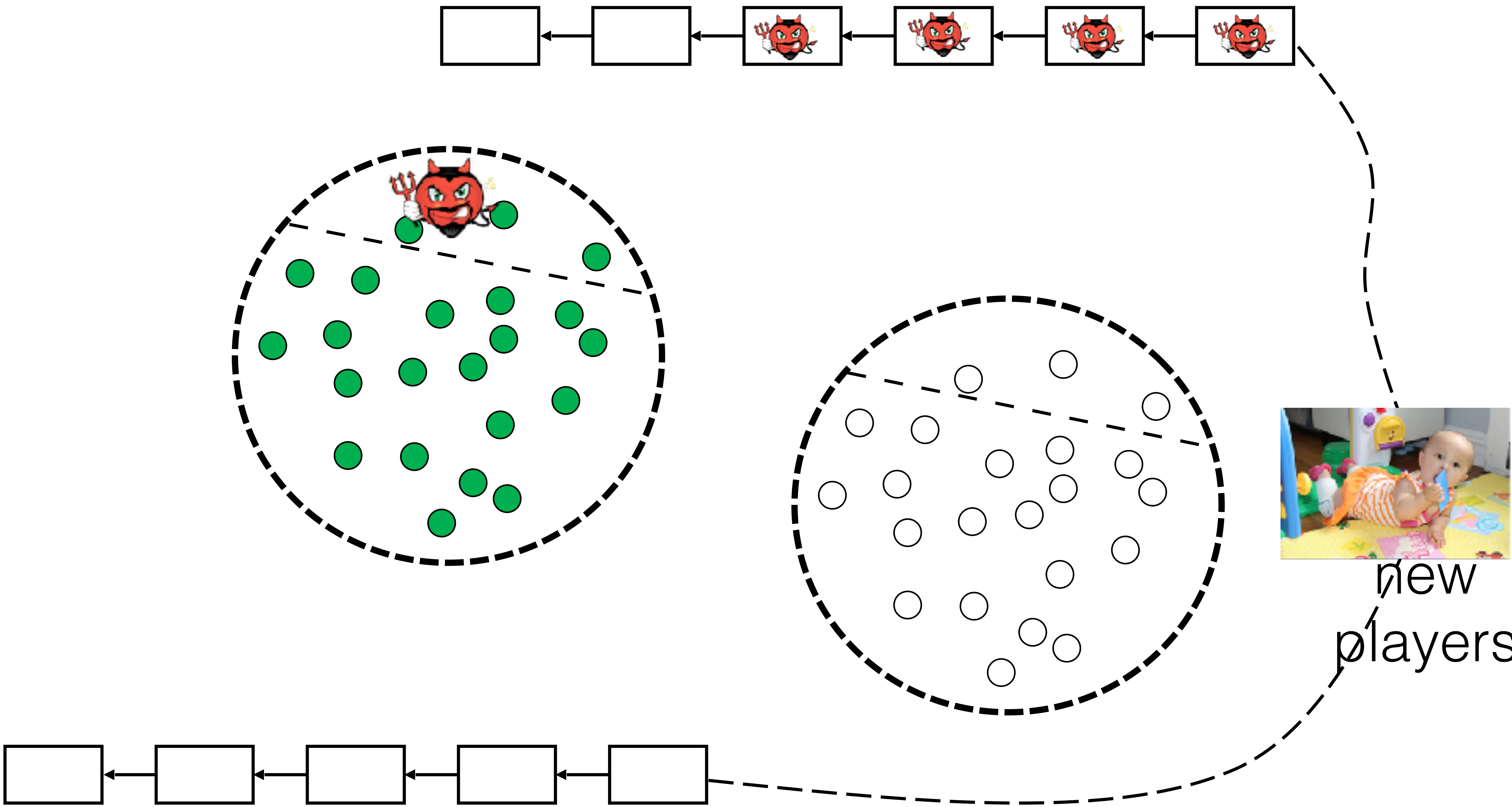
not a concern



splitting attack on a class of lightweight protocols



a big concern



However....main obstacle: splitting attack

Is that possible to fix the issue?

However….main obstacle: splitting attack

Is that possible to fix the issue?

Yes. players run a voting.

However….main obstacle: splitting attack

Is that possible to fix the issue?

Yes. players run a voting.

Voting is a conventional MPC, which cannot scale to a large network of nodes.

However....main obstacle: splitting attack

Is that possible to fix the issue?

However….main obstacle: splitting attack

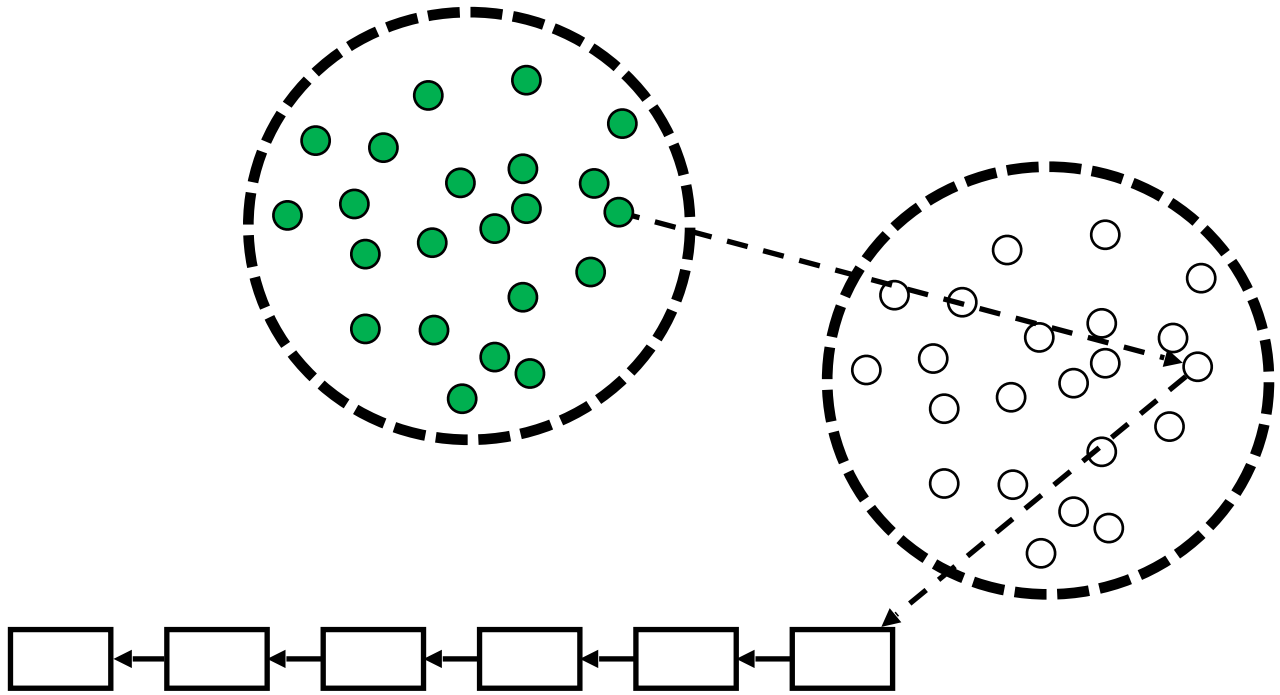
Is that possible to fix the issue?

Yes. via external checkpoints

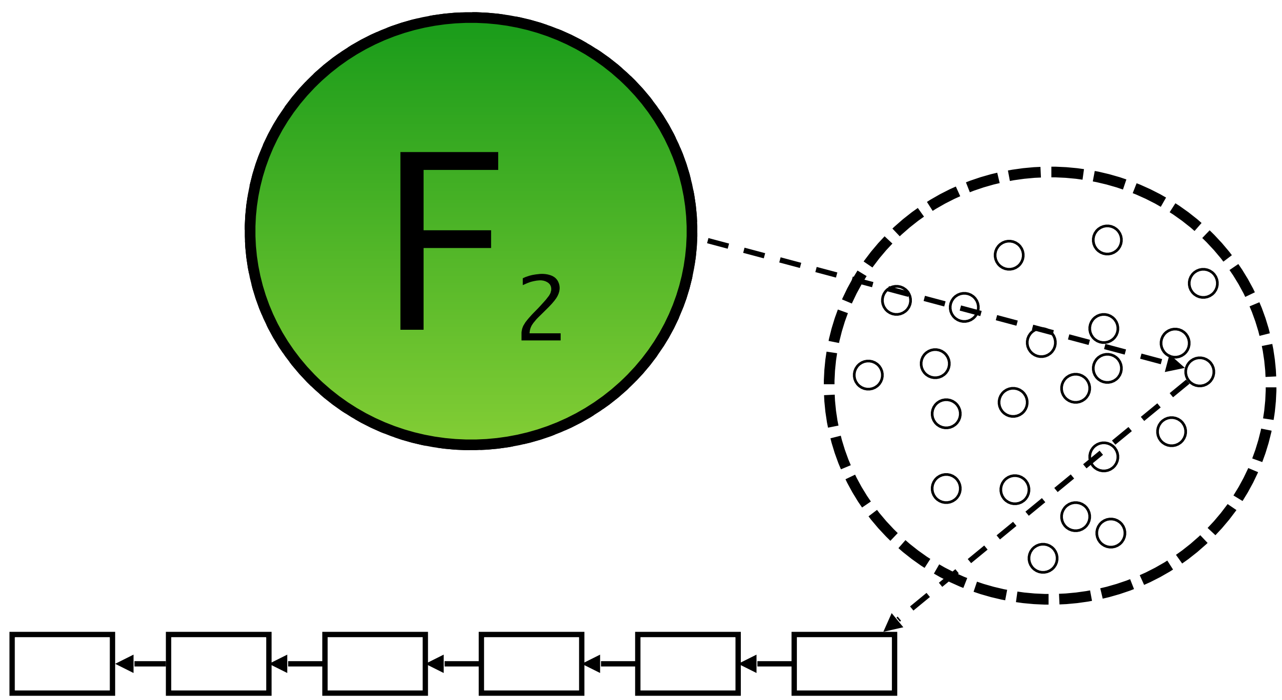
However....main obstacle:
splitting attack

Is that possible to fix the issue?
Yes. via external checkpoints

this violates the
decentralization.



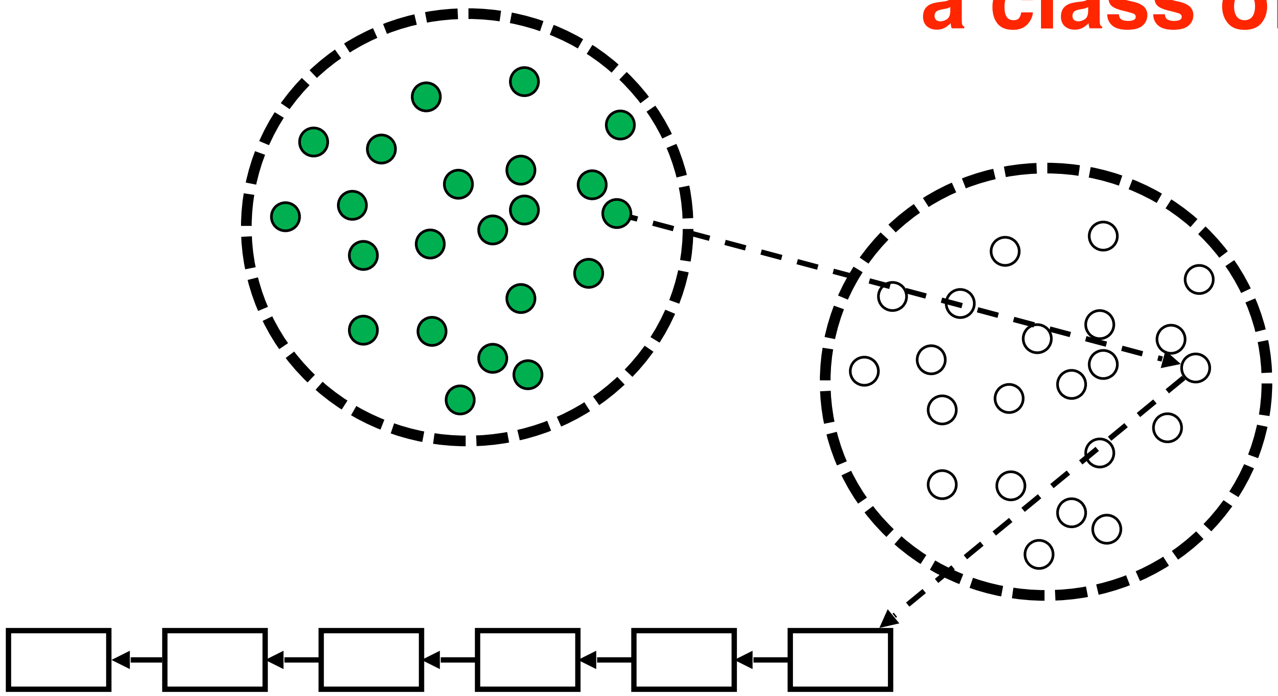
if we can design a lightweight protocol



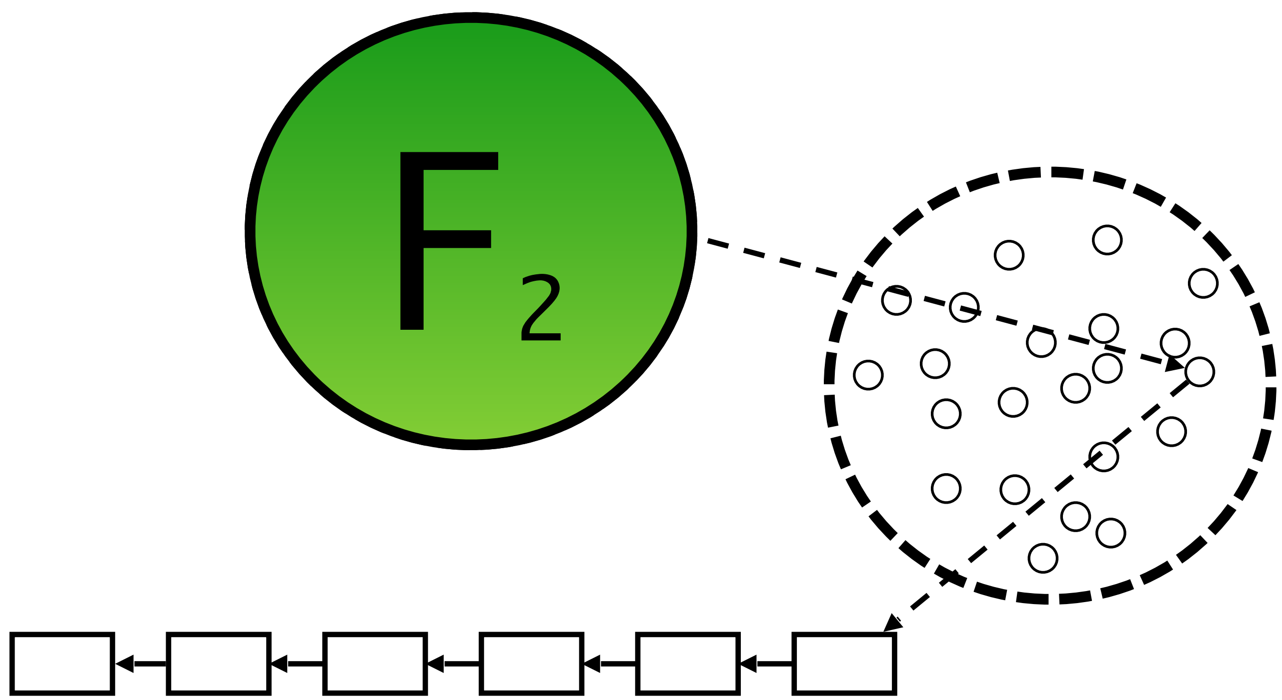
which achieves an *environment friendly* beacon functionality

then we could make a better blockchain than Nakamoto's

a class of lightweight protocols DO NOT



~~if we can design a lightweight protocol~~



which achieves an *environment friendly* beacon functionality

then we could make a better blockchain than Nakamoto's

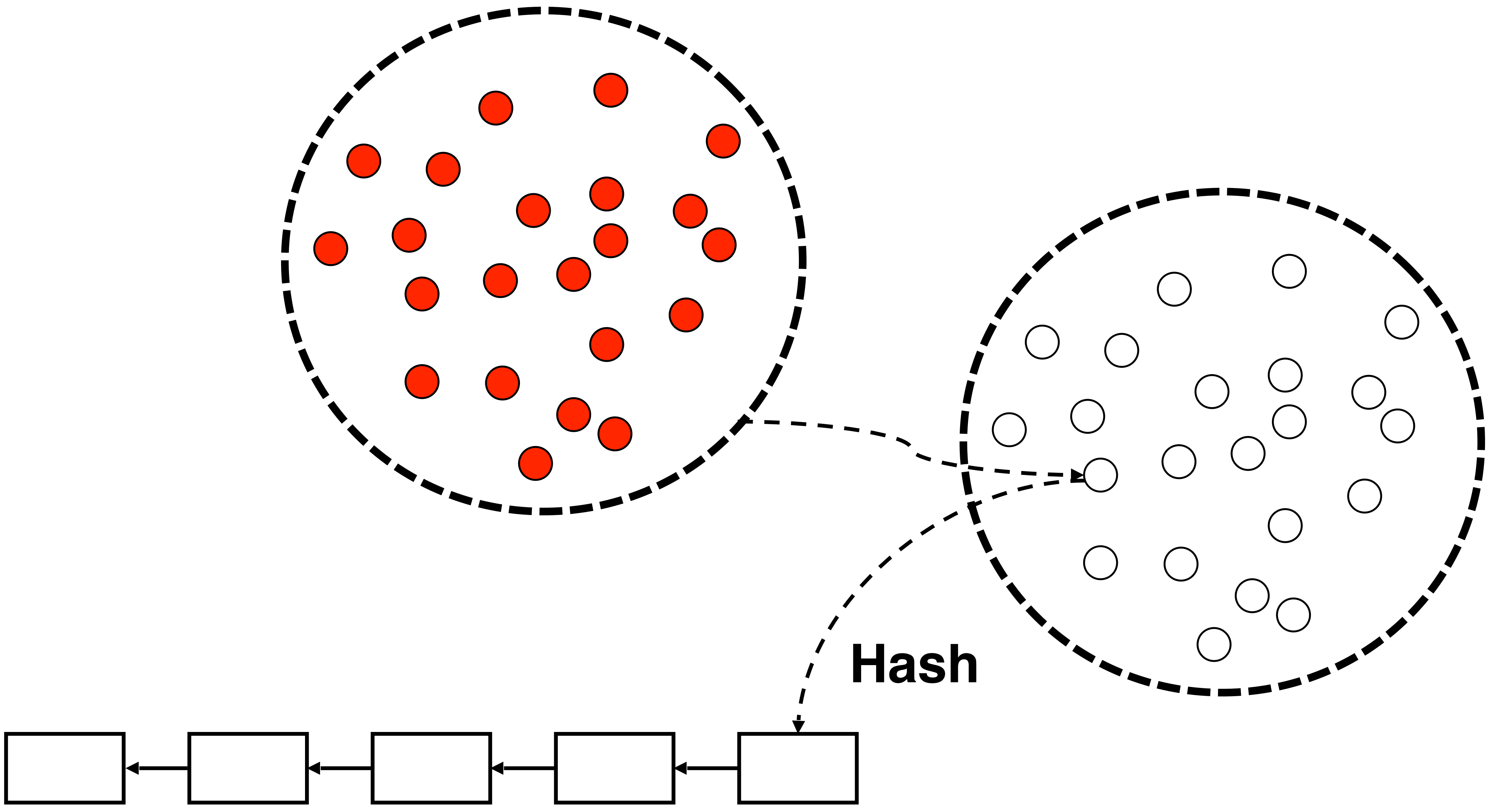
Interesting Question

- Proof-of-stake blockchain
  - open setting
  - Internet-scale
  - provably secure

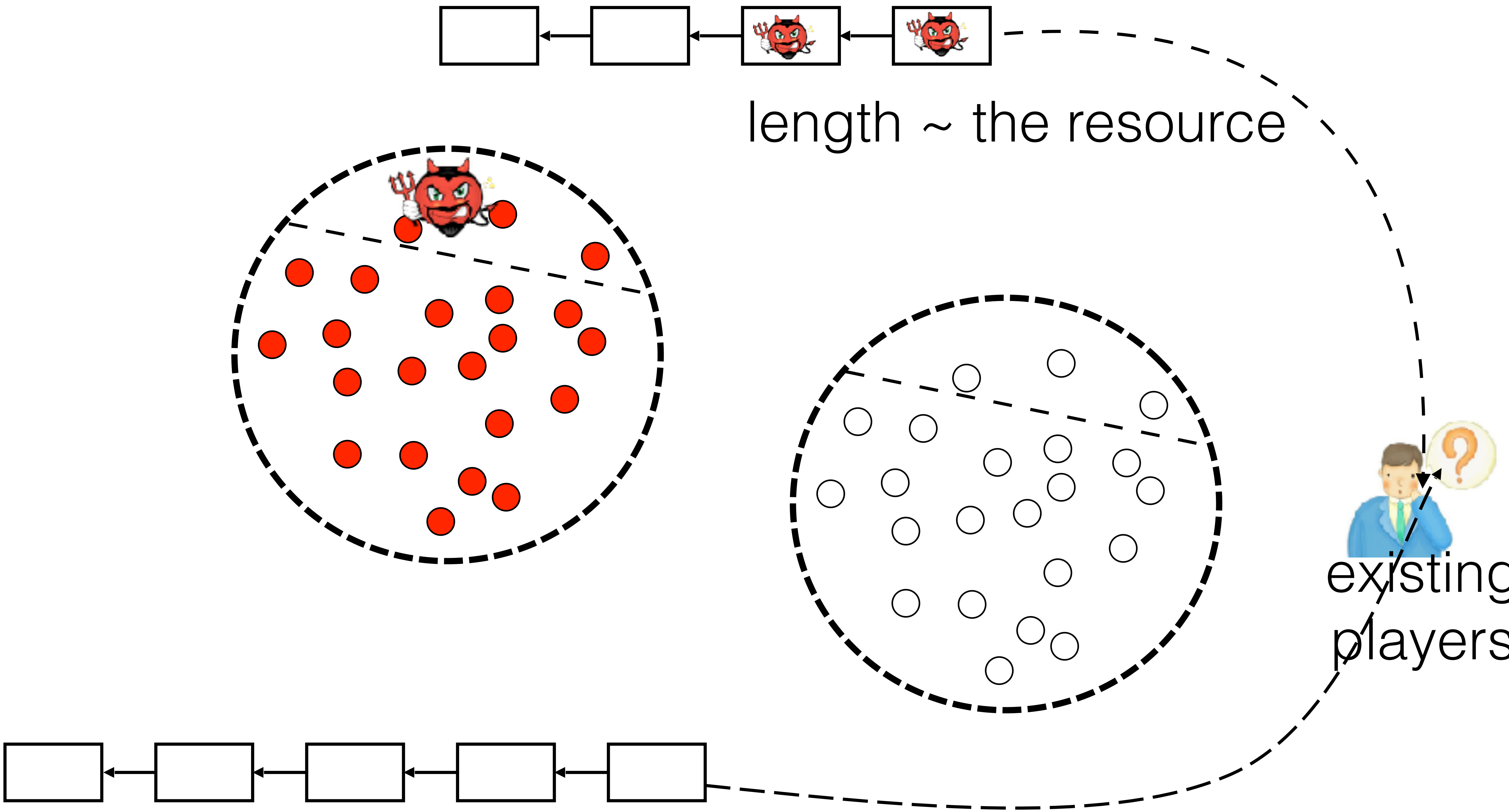
However….main obstacle: splitting attack

Is Nakamoto's design OK?

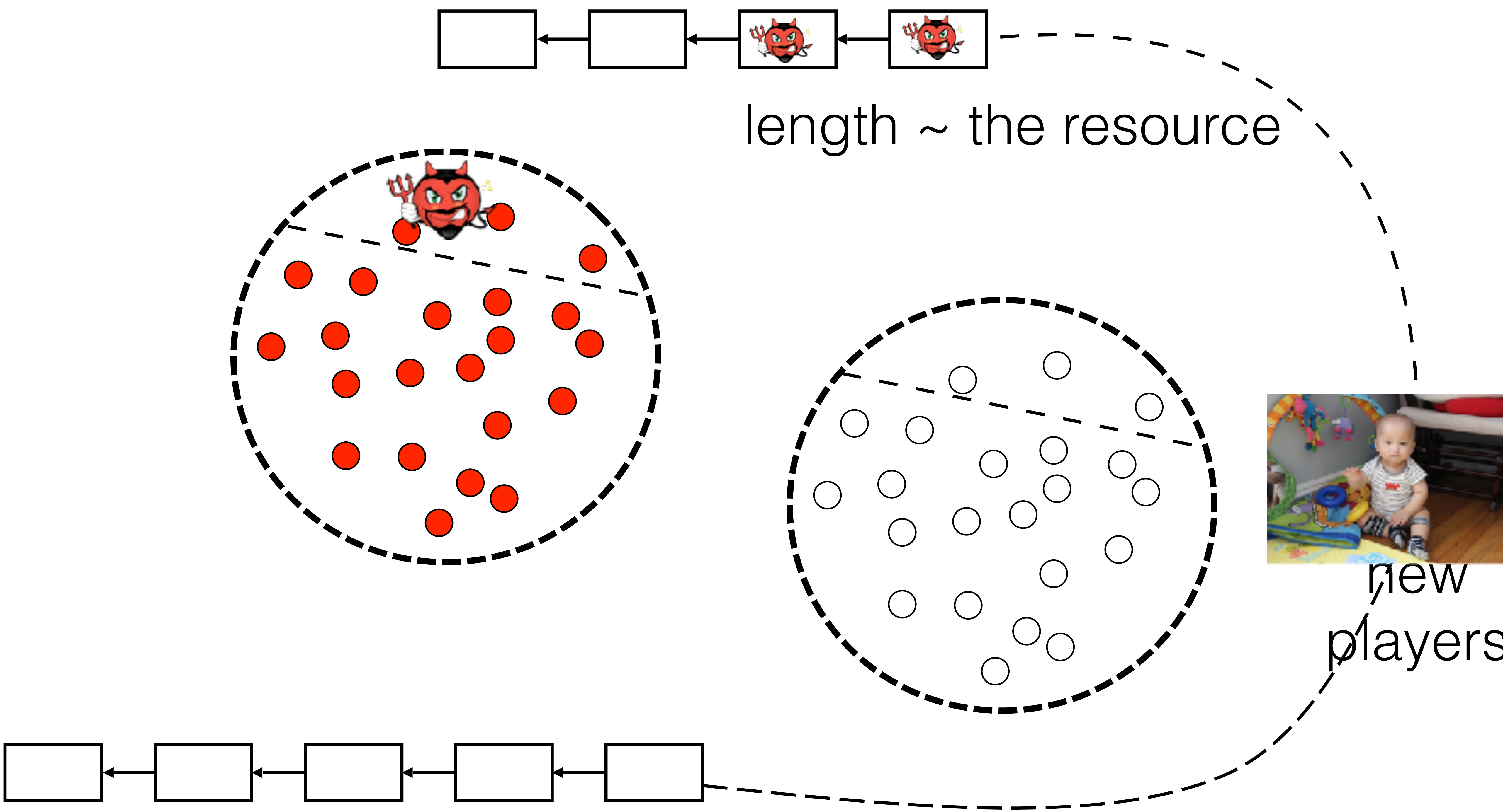
splitting attack on Nakamoto's design?

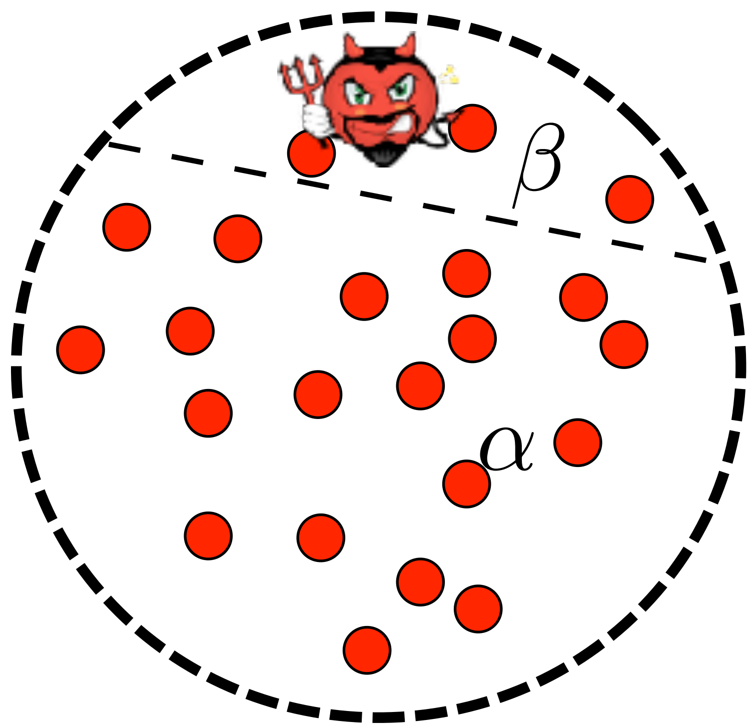


splitting attack on Nakamoto's design?

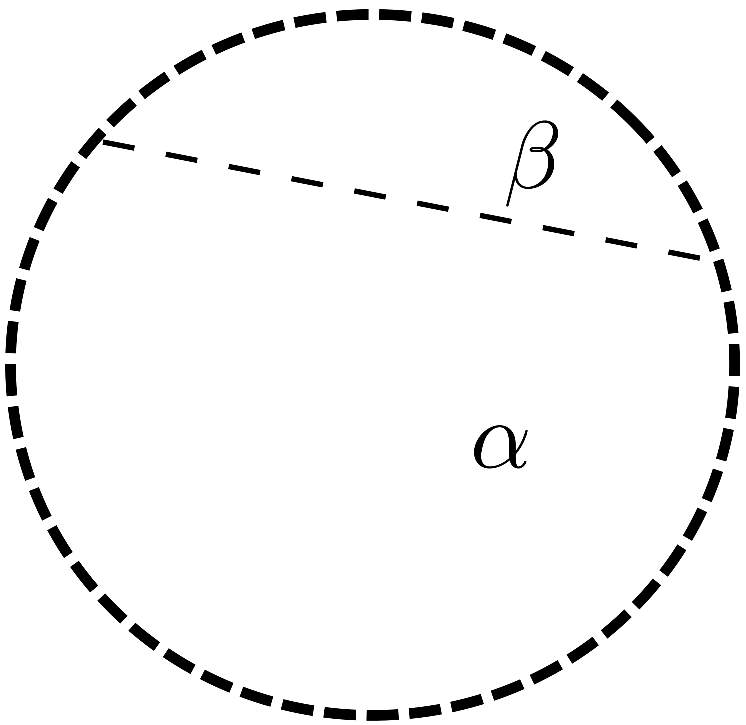


splitting attack on Nakamoto's design?





β
α


β
α

However….main obstacle: splitting attack

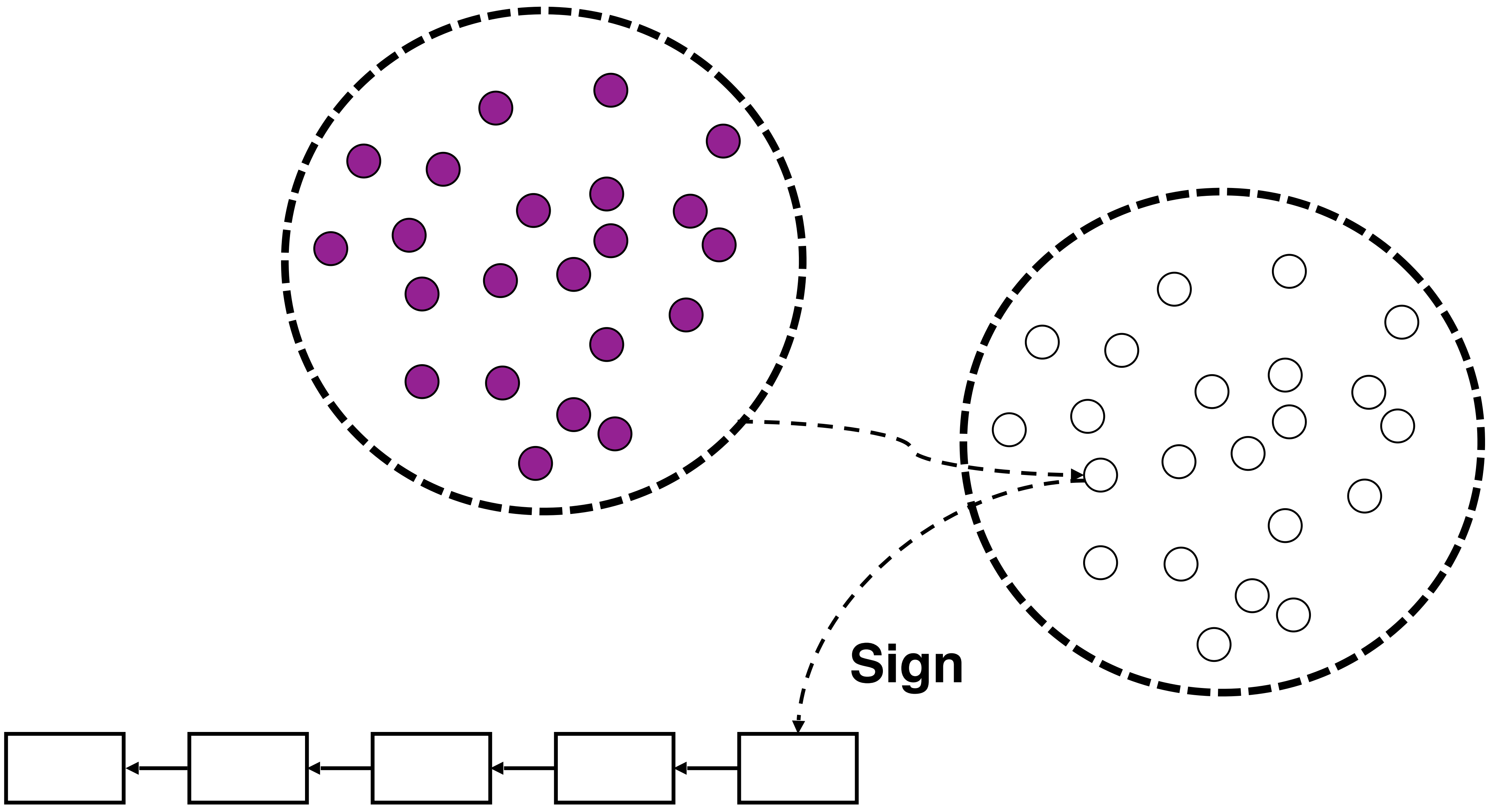
Is Nakamoto's design OK?

Yes.

However....main obstacle: splitting attack

Any other solutions against splitting attack?

trusted hardware based blockchains



However....main obstacle: splitting attack

Is this hardware based solution good?

However....main obstacle: splitting attack

Is this hardware based solution good?

Probably Not.
Trapdoor available to a single party

However....main obstacle: splitting attack

Any other solutions against splitting attack?

Yes. Proof of X

X={Work, trusted hardware, Storage, ... Human-work, ...}

Blocki, Zhou, Designing Proof of Human-work Puzzles for Cryptocurrency and Beyond. TCC 2016

However....main obstacle: splitting attack

Any other solutions against splitting attack?

Yes. Proof of X

X={Work, trusted hardware, Storage, ... Human-work, ...}
useful work, combining work with storage, memory hard PoW

Are they good?

References

- Modeling idea:
  Garay, Kiayias, Zhou, CSF 10
- Proof-of-Stake:
  Algorand; Ouroboros; Snow White;
- Proof-of-X:
  PoET; SpaceMint; PermaCoin; PrimeCoin; PoST; memory hard PoW;

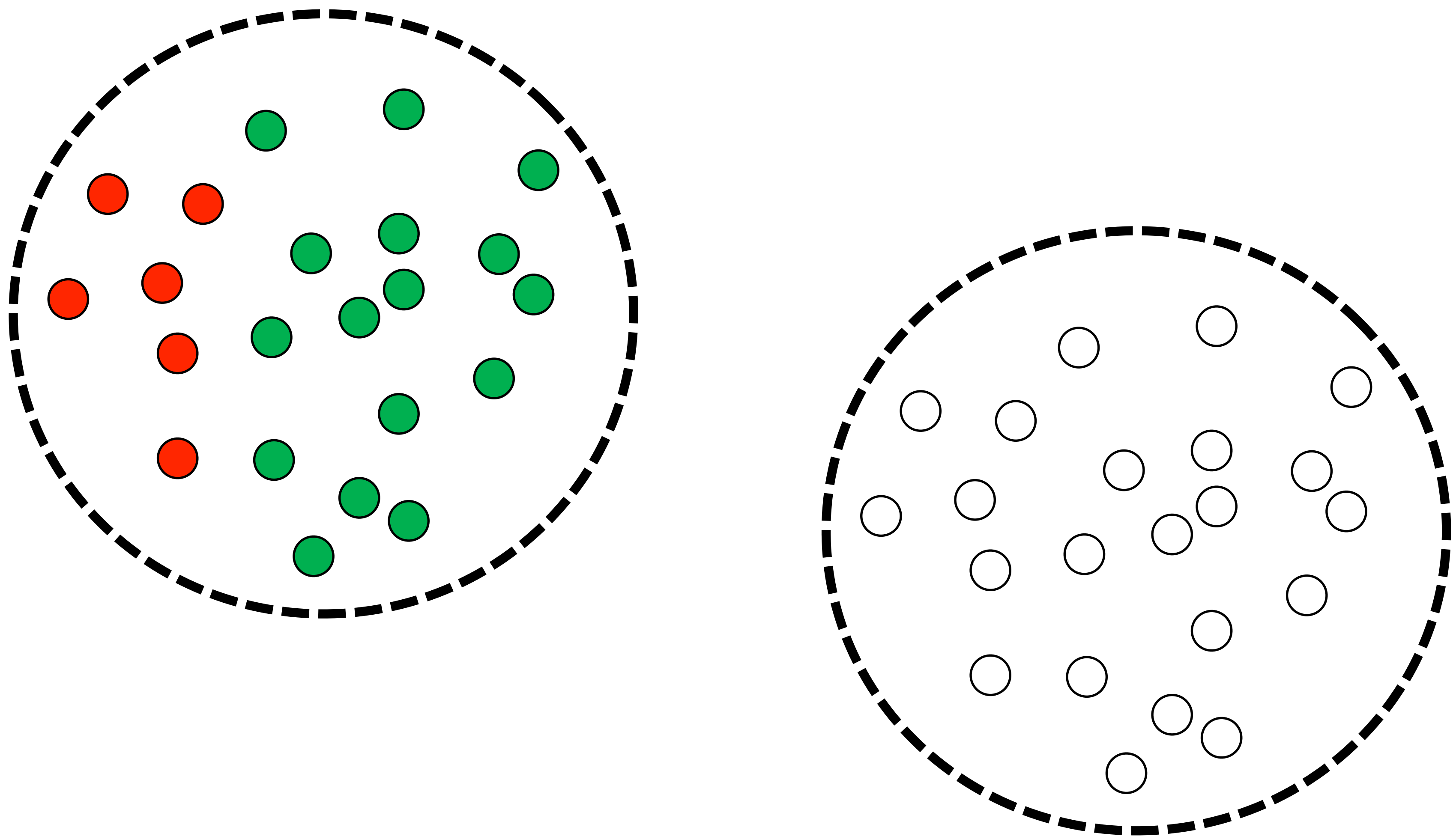
Alternative Mechanisms

A Design Example: 2-hop Blockchain

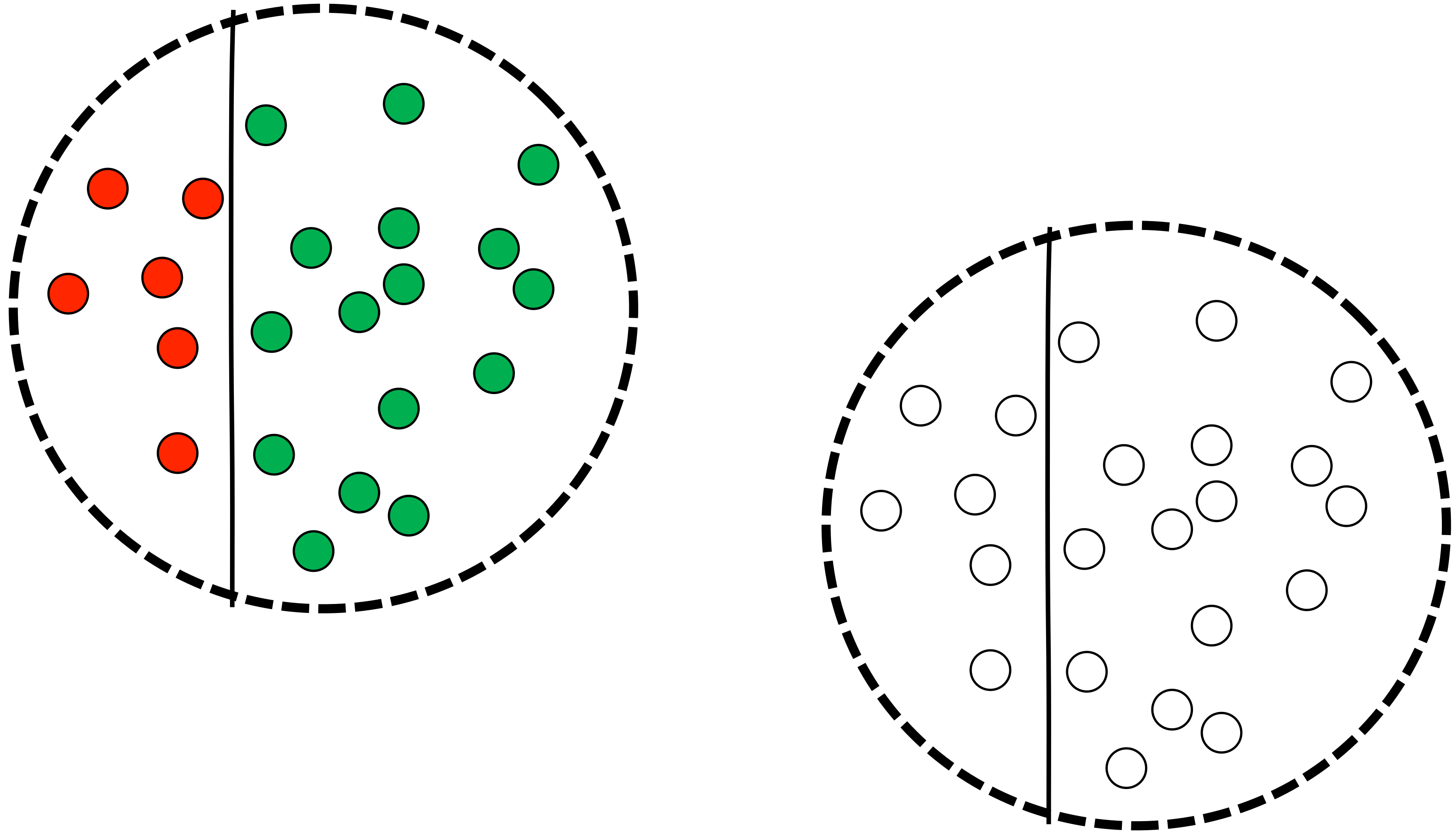
so far

- a unified view for constructing (a class of) open blockchains has been developed
- existing proof-of-stake based open blockchains **cannot** scale to a large number of nodes

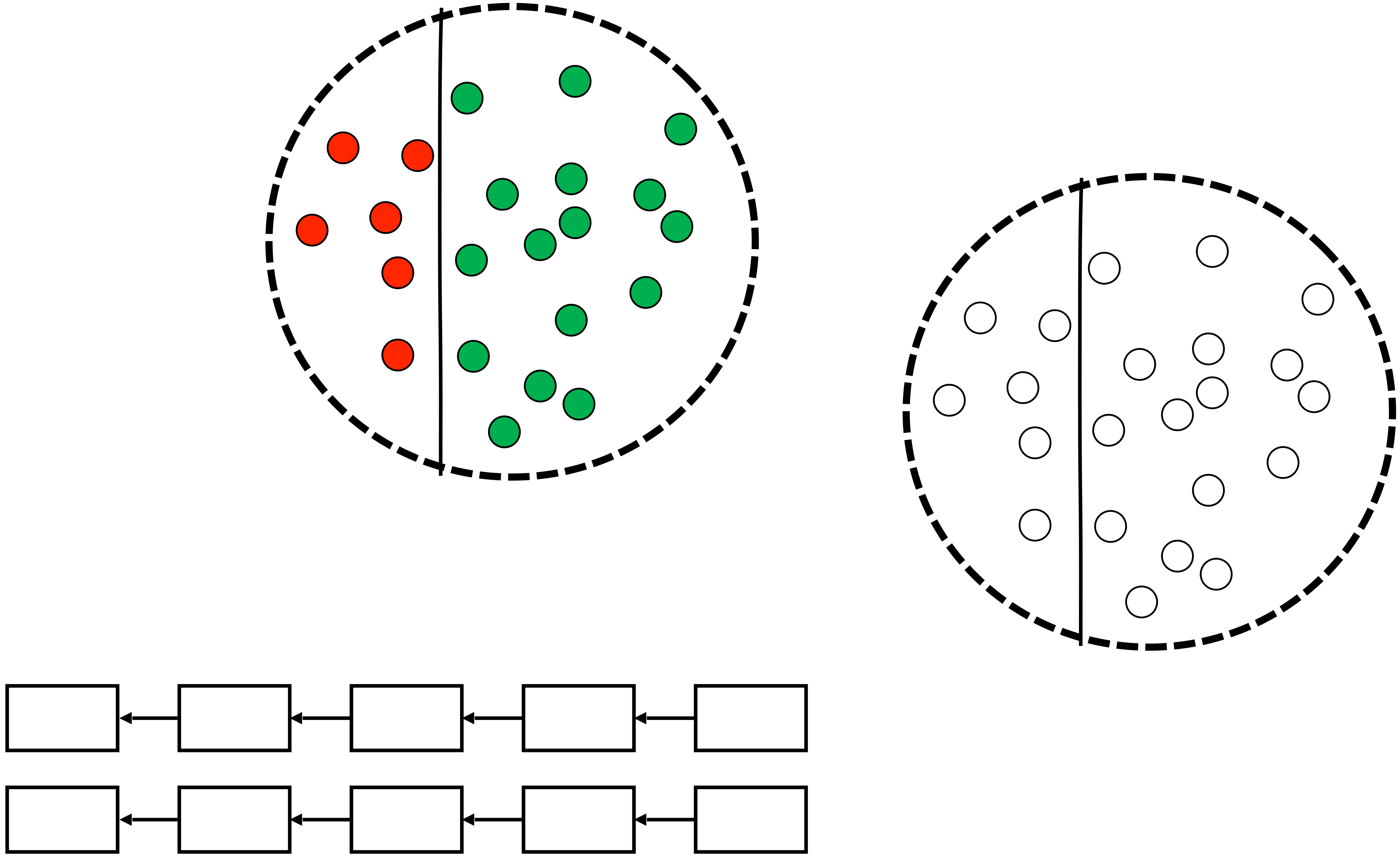
PoW/PoS-based Blockchain



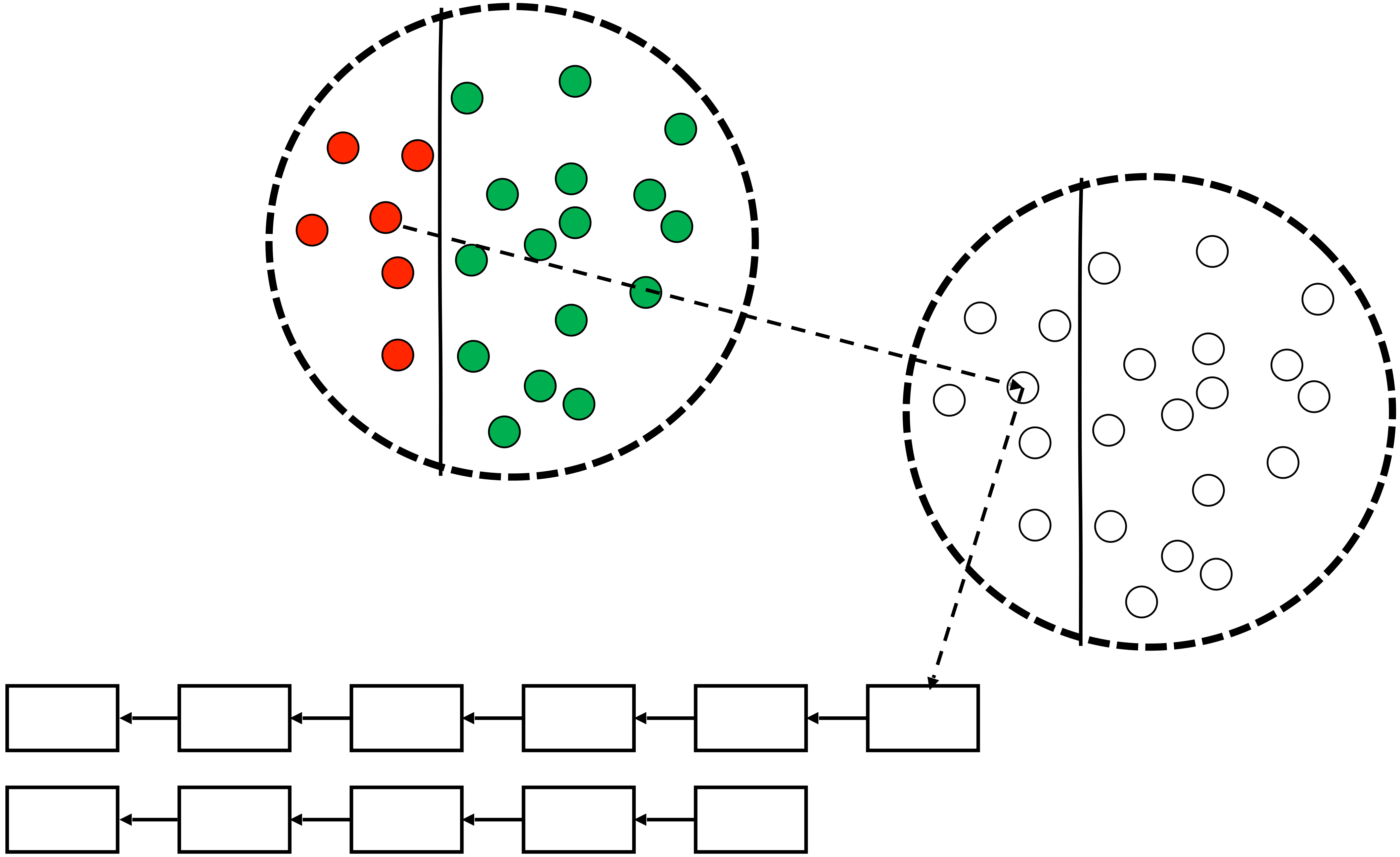
PoW/PoS-based Blockchain



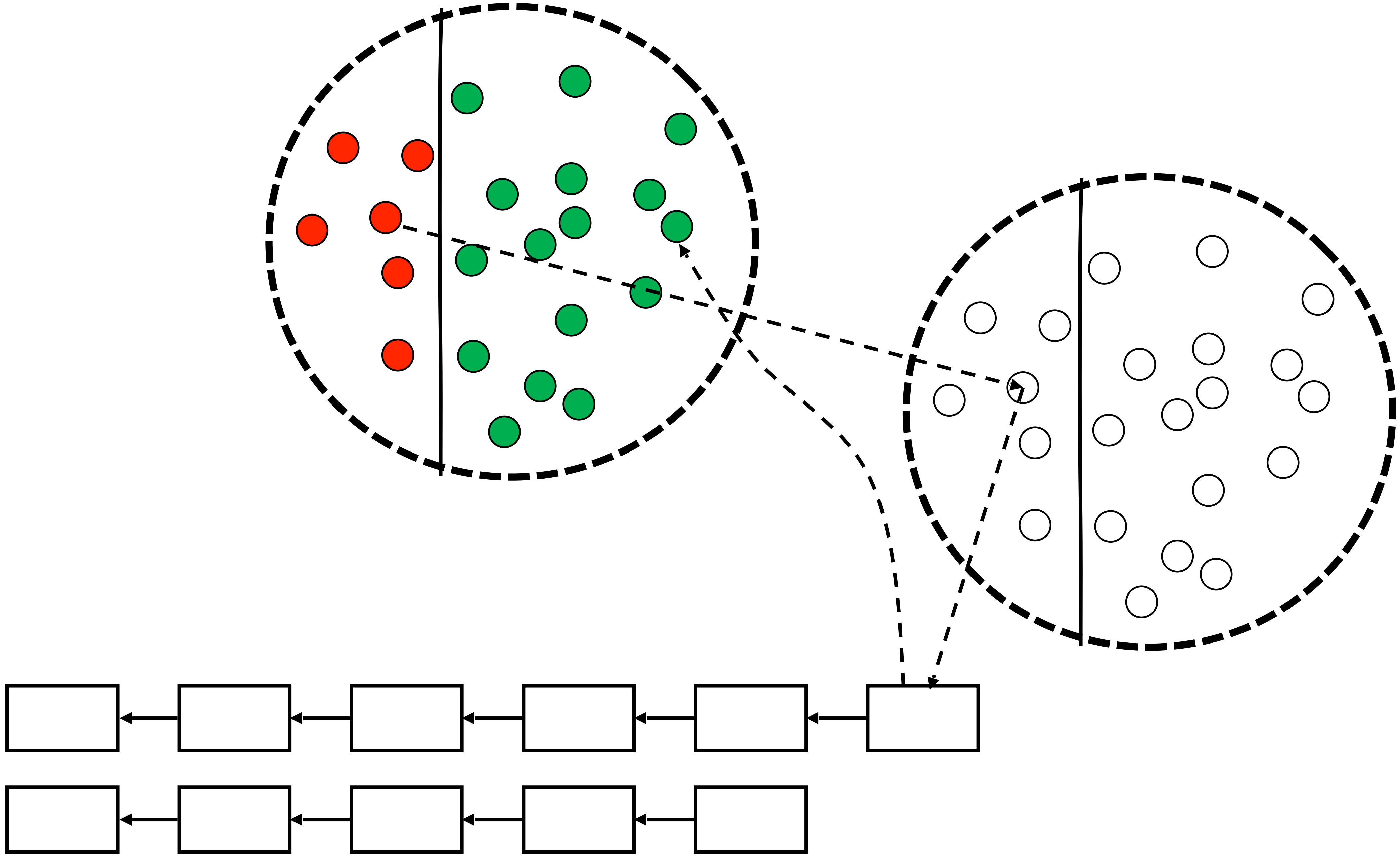
PoW/PoS-based Blockchain



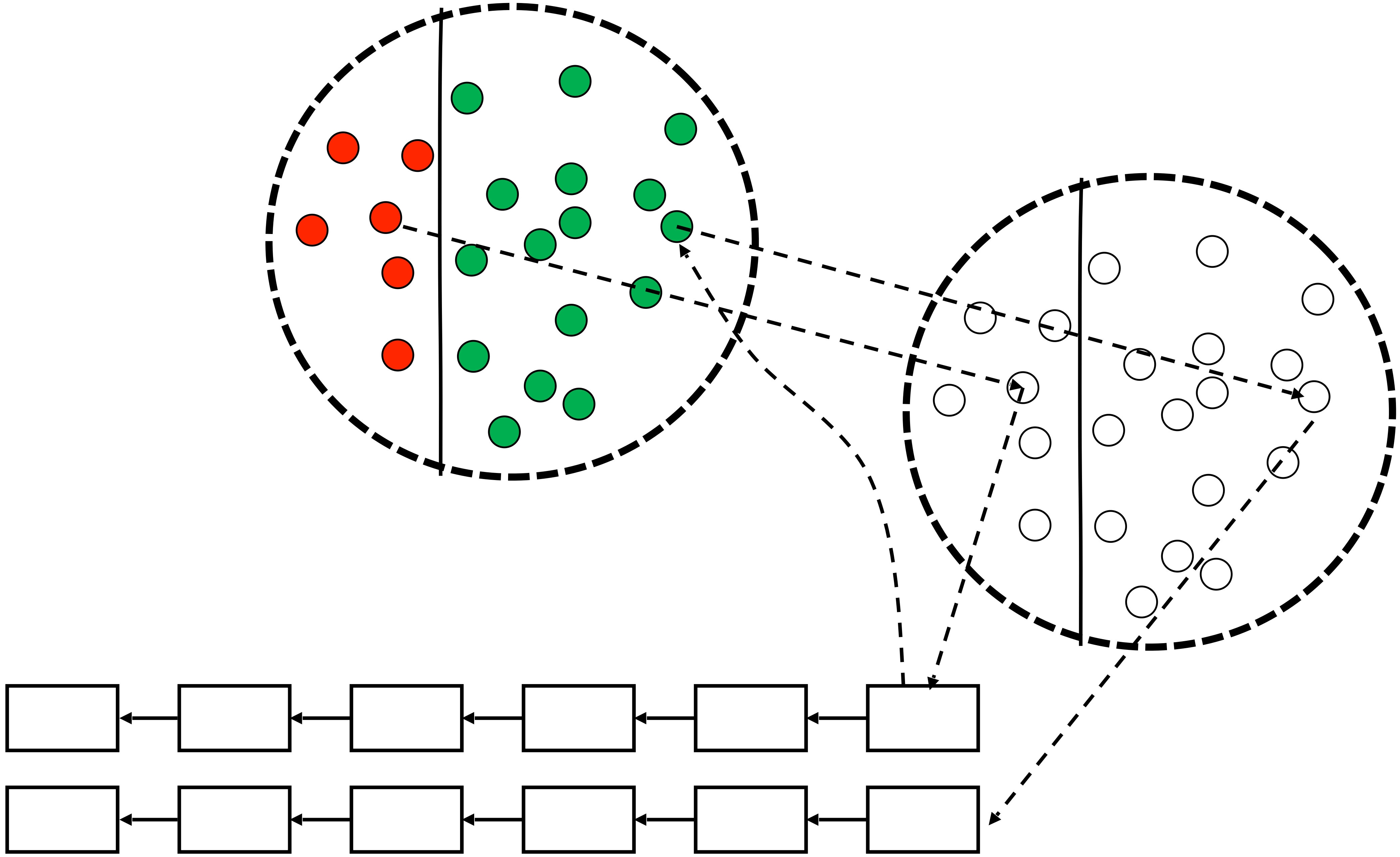
PoW/PoS-based Blockchain



PoW/PoS-based Blockchain

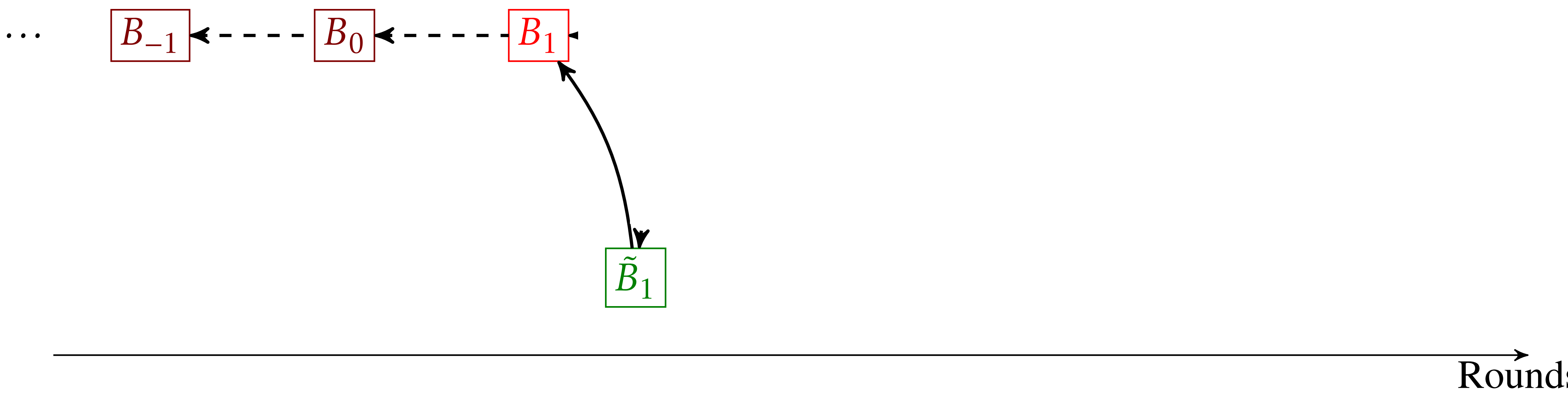


PoW/PoS-based Blockchain



2-hop blockchain

[Duong,Fan,**Z**.,16]

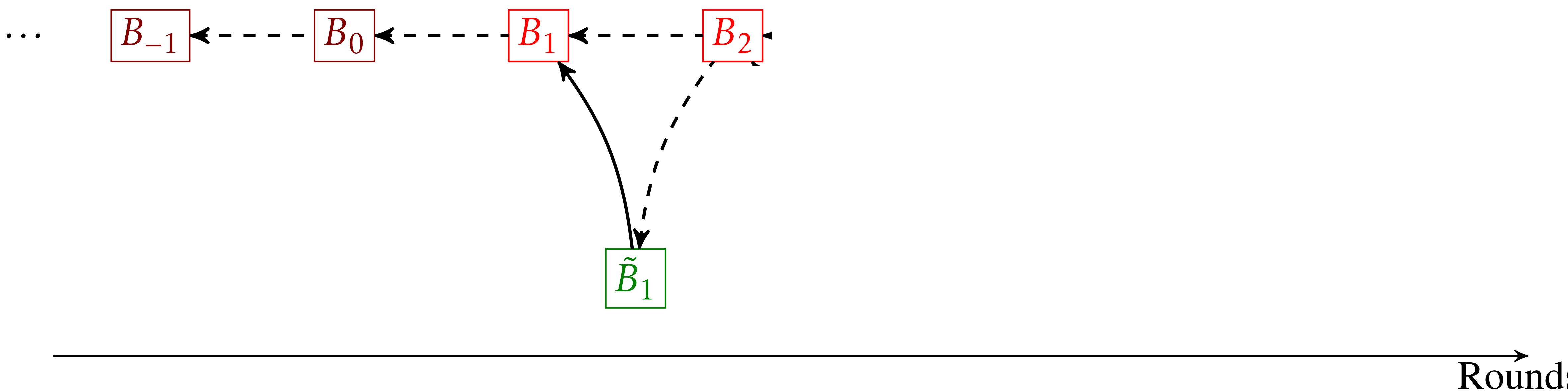


$$H(B_1 || \tilde{B}_1 || nonce_1) < \mathtt{T}$$

Duong, Fan, Zhou, 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely. IACR ePrint 2016

2-hop blockchain

[Duong,Fan,**Z**.,16]

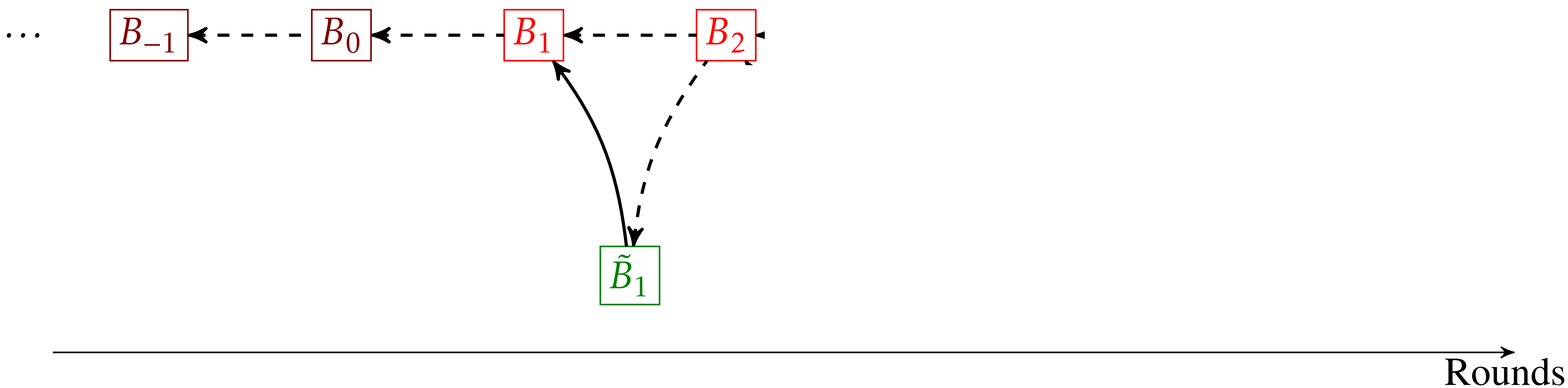


$$H(B_1||\tilde{B}_1||nonce_1) < \mathtt{T}$$

Duong, Fan, Zhou, 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely. IACR ePrint 2016

2-hop blockchain

[Duong,Fan,**Z.**,16]

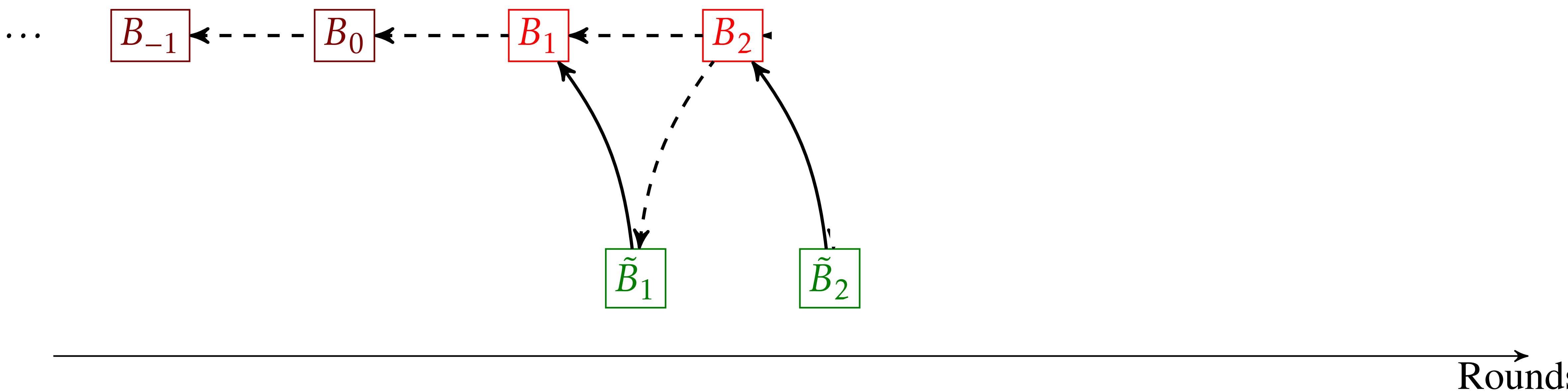


$$H(B_1||\tilde{B}_1||nonce_1) < \mathtt{T} \qquad \tilde{H}(B_2||\tilde{\mathsf{vk}}_2) < \tilde{\mathtt{T}}$$

Duong, Fan, Zhou, 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely. IACR ePrint 2016

2-hop blockchain

[Duong,Fan,**Z.**,16]



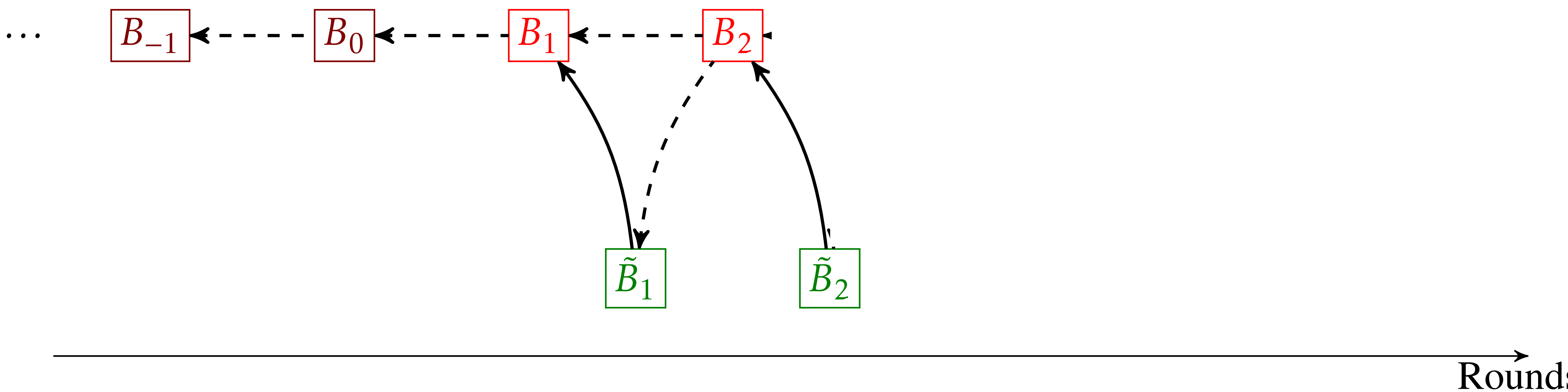
$$H(B_1 || \tilde{B}_1 || nonce_1) < \mathtt{T}$$

$$\tilde{H}(B_2 || \tilde{\mathsf{vk}}_2) < \tilde{\mathtt{T}}$$

Duong, Fan, Zhou, 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely. IACR ePrint 2016

2-hop blockchain

[Duong,Fan,**Z.**,16]



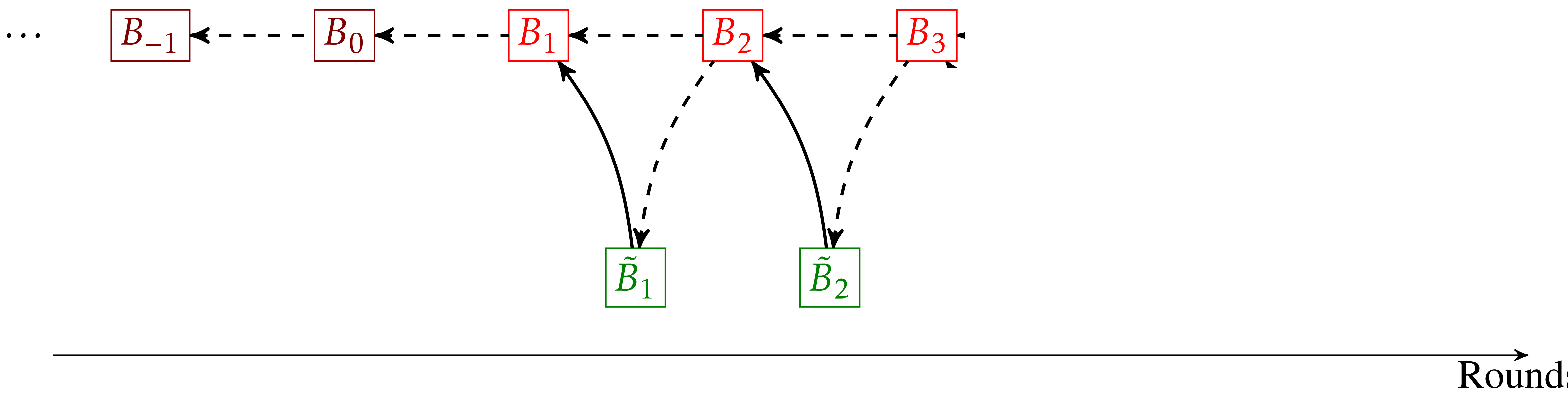
$$H(B_1||\tilde{B}_1||nonce_1) < \mathtt{T}$$
$$H(B_2||\tilde{B}_2||nonce_2) < \mathtt{T}$$

$$\tilde{H}(B_2||\tilde{\mathsf{vk}}_2) < \tilde{\mathtt{T}}$$

Duong, Fan, Zhou, 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely. IACR ePrint 2016

2-hop blockchain

[Duong,Fan,**Z.**,16]



$$H(B_1||\tilde{B}_1||nonce_1) < \mathtt{T}$$

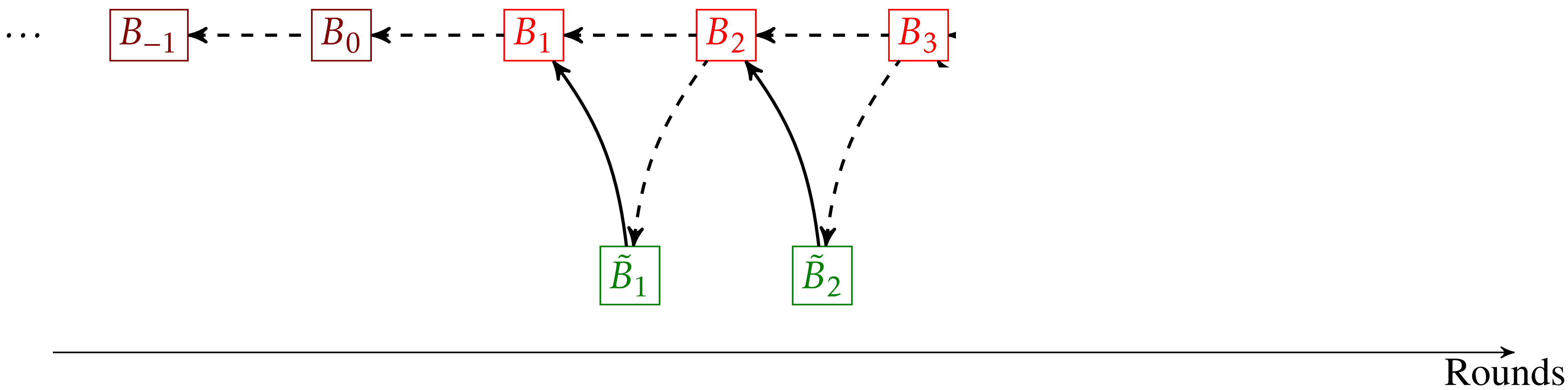
$$H(B_2||\tilde{B}_2||nonce_2) < \mathtt{T}$$

$$\tilde{H}(B_2||\tilde{\mathsf{vk}}_2) < \tilde{\mathtt{T}}$$

Duong, Fan, Zhou, 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely. IACR ePrint 2016

2-hop blockchain

[Duong,Fan,**Z.**,16]



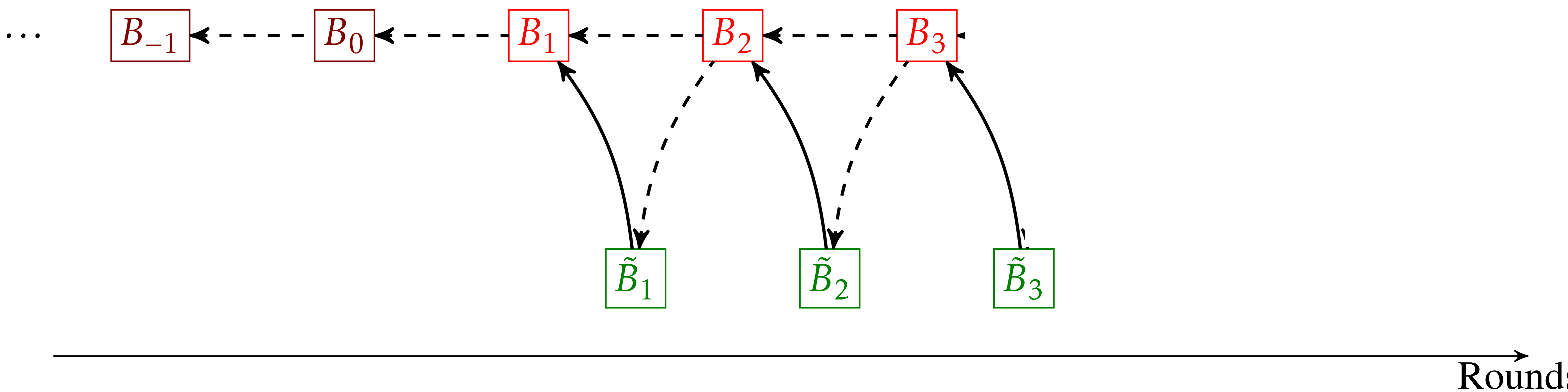
$$H(B_1||\tilde{B}_1||nonce_1) < \mathtt{T} \qquad \tilde{H}(B_2||\tilde{\mathsf{vk}}_2) < \tilde{\mathtt{T}}$$

$$H(B_2||\tilde{B}_2||nonce_2) < \mathtt{T} \qquad \tilde{H}(B_3||\tilde{\mathsf{vk}}_3) < \tilde{\mathtt{T}}$$

Duong, Fan, Zhou, 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely. IACR ePrint 2016

2-hop blockchain

[Duong,Fan,**Z**.,16]



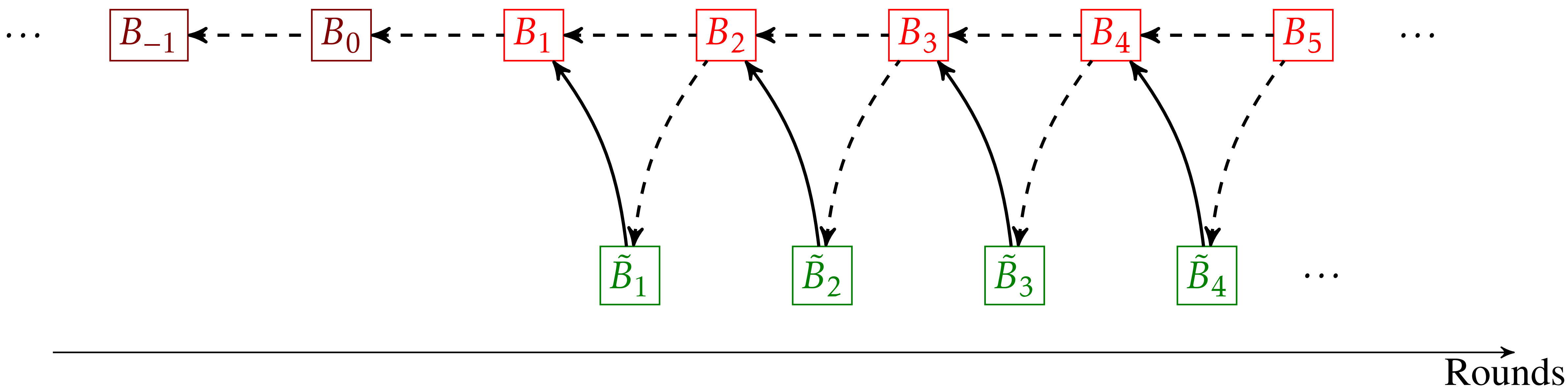
$$H(B_1 || \tilde{B}_1 || nonce_1) < \mathtt{T}$$
$$H(B_2 || \tilde{B}_2 || nonce_2) < \mathtt{T}$$

$$\tilde{H}(B_2 || \tilde{\mathsf{vk}}_2) < \tilde{\mathtt{T}}$$
$$\tilde{H}(B_3 || \tilde{\mathsf{vk}}_3) < \tilde{\mathtt{T}}$$

Duong, Fan, Zhou, 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely. IACR ePrint 2016

2-hop blockchain

[Duong,Fan,**Z.**,16]

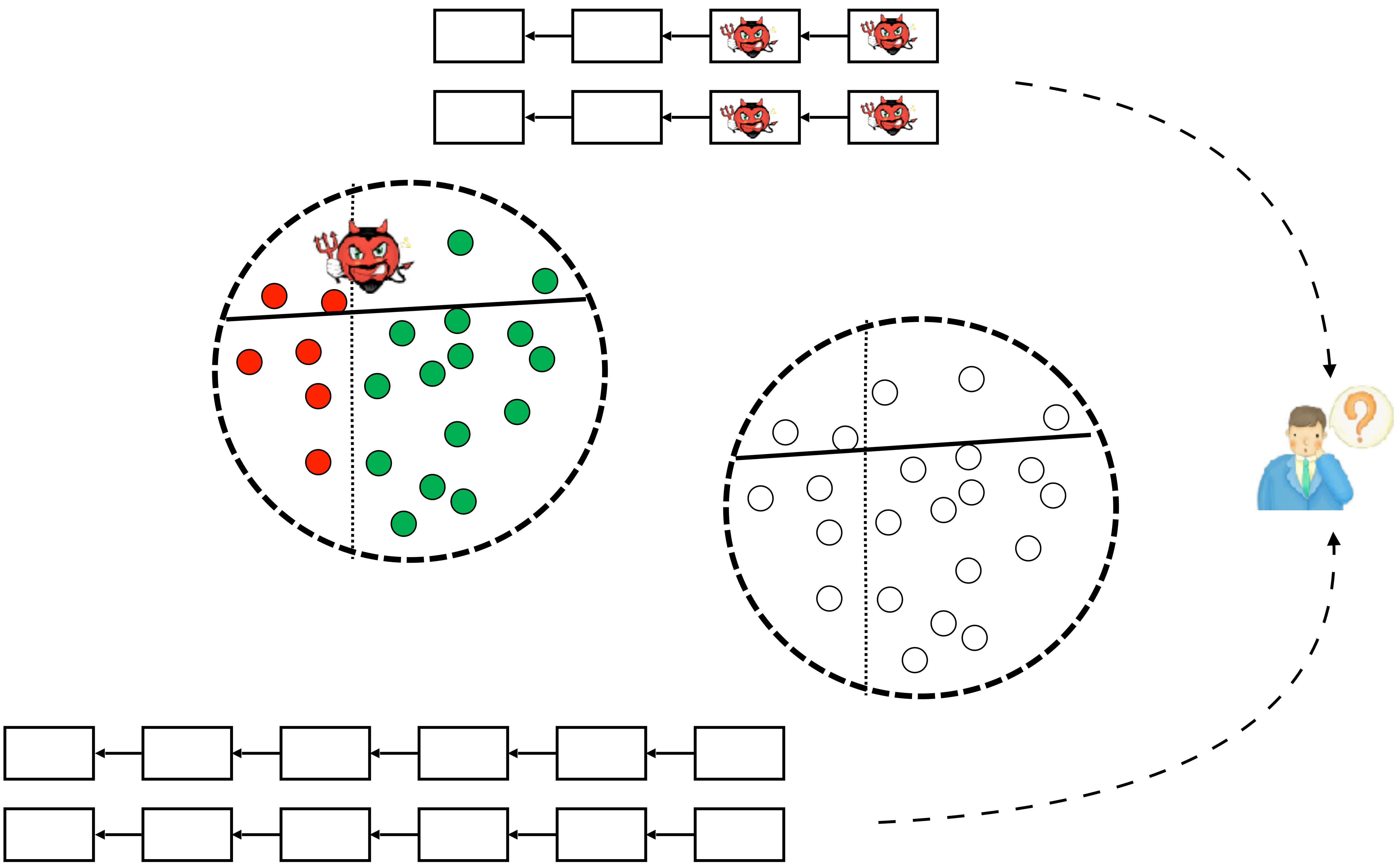


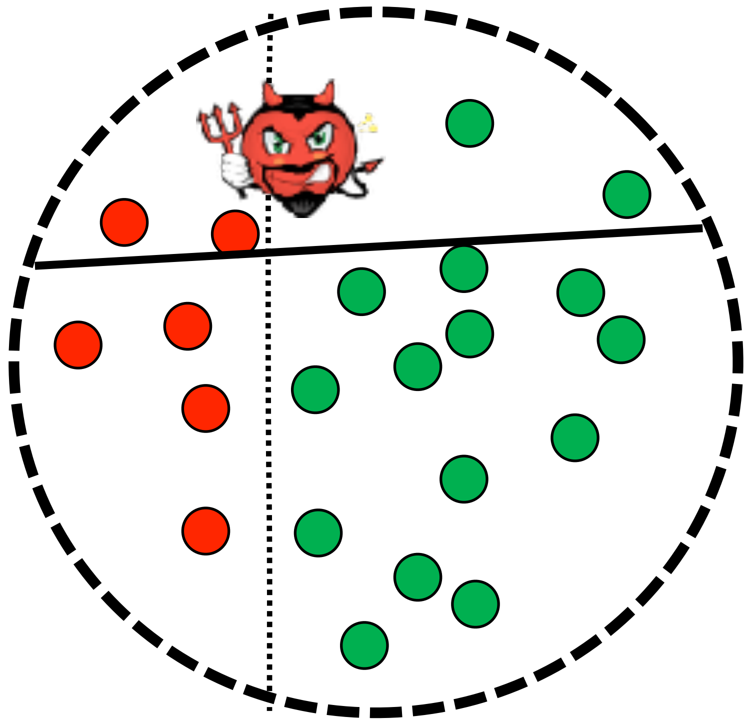
$$H(B_1||\tilde{B}_1||nonce_1) < \mathtt{T} \qquad \tilde{H}(B_2||\tilde{\mathsf{vk}}_2) < \tilde{\mathtt{T}}$$

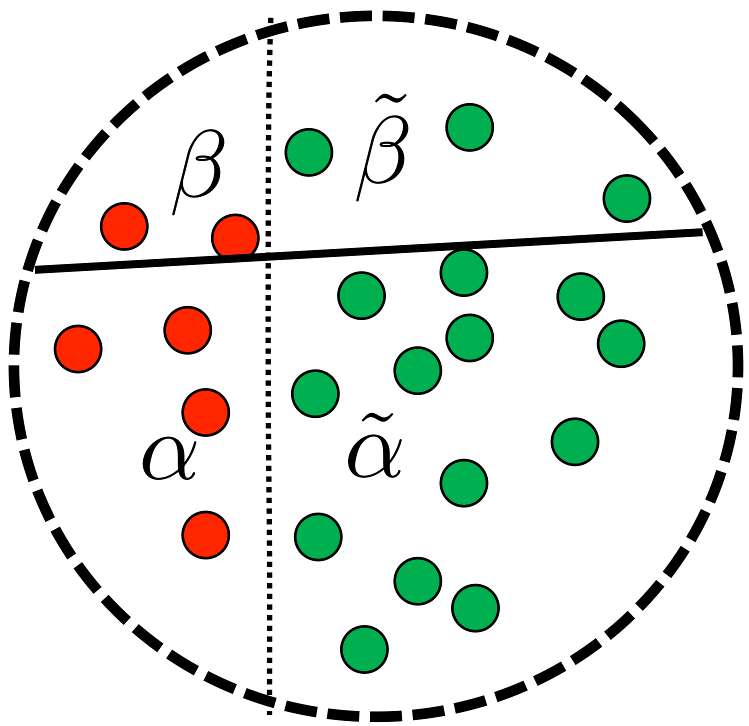
$$H(B_2||\tilde{B}_2||nonce_2) < \mathtt{T} \qquad \tilde{H}(B_3||\tilde{\mathsf{vk}}_3) < \tilde{\mathtt{T}}$$

Duong, Fan, Zhou, 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely. IACR ePrint 2016

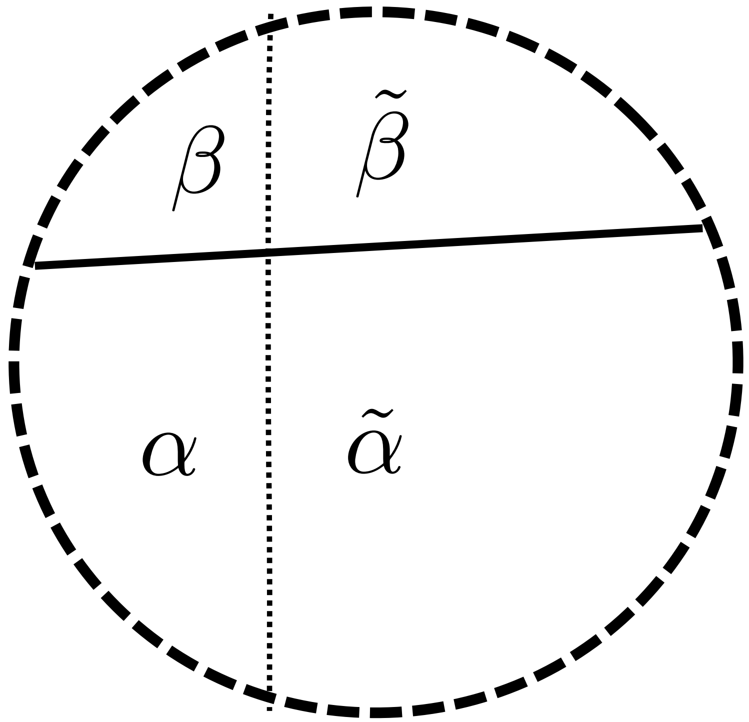
PoW/PoS-based Blockchain







β
$\tilde{\beta}$
α
$\tilde{\alpha}$



$$\hat{\beta} = \beta\tilde{\beta}$$

$$\hat{\alpha} = \alpha\tilde{\alpha}$$

$$\hat{\beta} < \hat{\alpha}$$

2-hop Blockchain

[Duong,Fan,**Z**.,16]

- Scalable to a huge network of nodes

- provably secure

V.0

2-hop Blockchain

[Duong,Fan,**Z**.,16]

- Scalable to a huge network of nodes
- provably secure

51% Honest Mining Power Assumption could be challenged

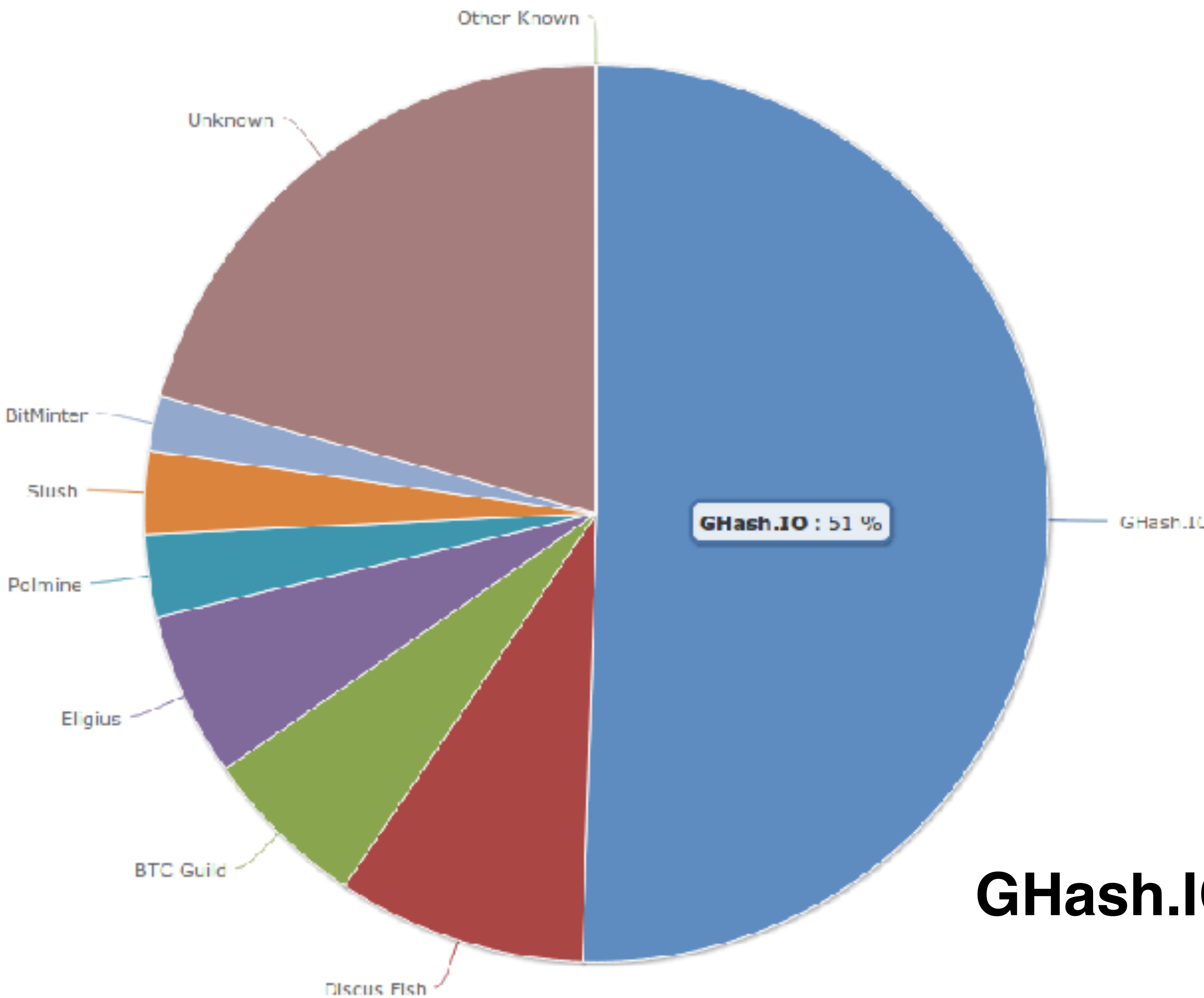
What about dedicated hardware?

黑科技

each new technique may have two sides

a breakthrough in certain area may be a big disaster in other areas

51% Honest Mining Power Assumption could be challenged



June 12, 2014
GHash.IO large mining pool crisis

All top mining pools are in China!

They might collude for whatever reason

V.1

TwinsChain

[Chepurnoy,Duong,Fan,**Z**.,16]

- Scalable to a huge network of nodes
- provably secure
- adaptive difficulty adjustment
- implementation

- adaptive difficulty adjustment

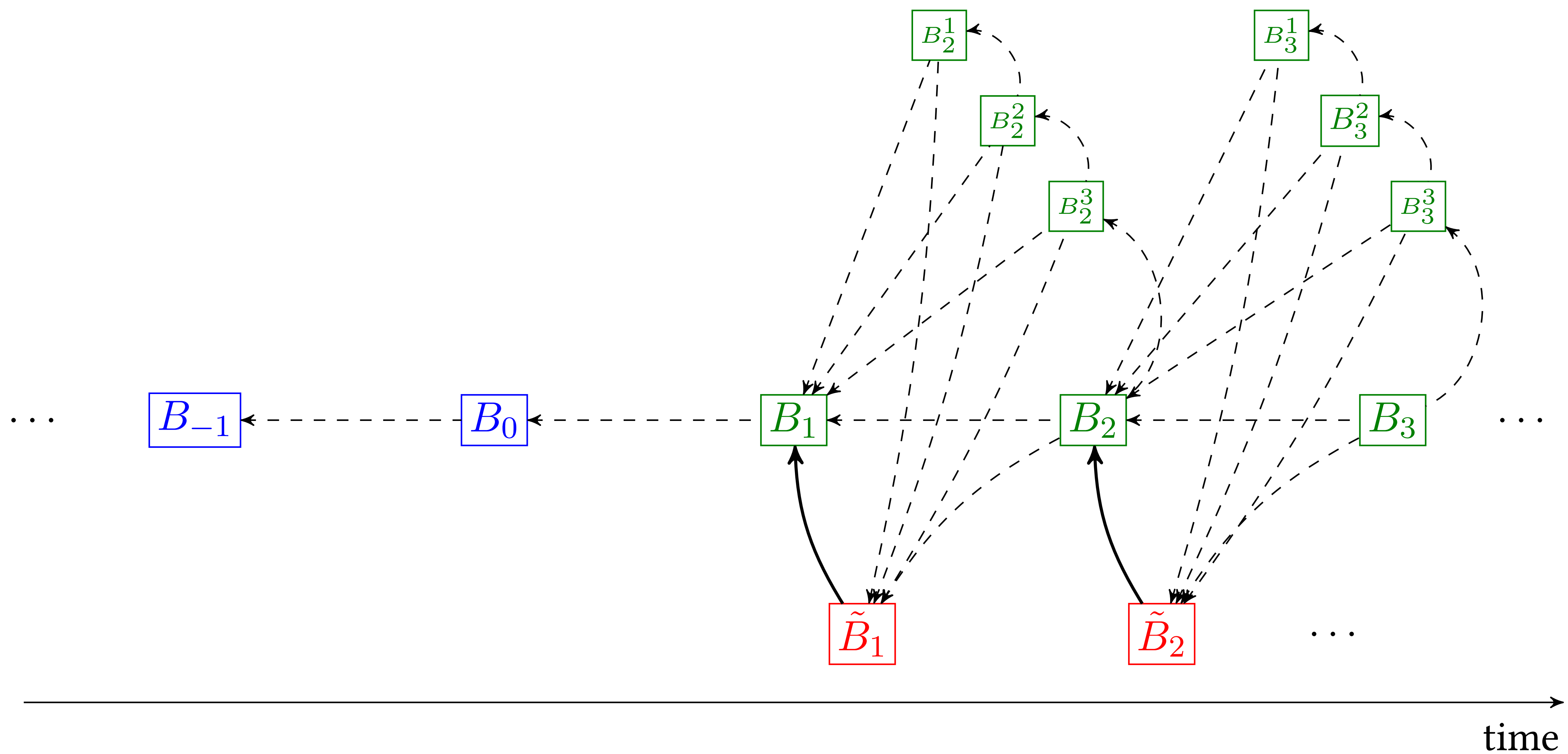


Figure 2: TwinsChain blockchain structure

Here, dot arrows (that link to the previous successful block and attempting blocks) denote the first hops, and solid arrows denote the second hops. Green blocks B_i's denote the successful proof-of-work blocks, B_i^j's denote the attempting proof-of-work blocks, and red blocks $\tilde{B}_i$'s denote the corresponding proof-of-stake blocks. Note that the blue blocks are from the "mature blockchain".

Atlassian, Inc.

Inbox (2,268) - hszhou@vcu.edu - Virginia C... | Bitcoin Summer School 2016 | Cryptology ePrint Archive: Recent Updates | twinscoin / twinschain

Bitbucket Teams Projects Repositories Snippets

twinschain

ACTIONS

- Clone
- Compare
- Fork

NAVIGATION

- Overview
- Source
- Commits
- Branches
- Pull requests
- Downloads

twinschain / twinschain

Overview

https://bitbucket.org/twinscoin/twinschain

Last updated	2016-11-11
Language	—
Access level	Read

1 Branch, 0 Tags, 0 Forks, 1 Watcher

TwinsChain Implementation

Building

The following instruction are for Linux environment only.

1. First, you need to install Java. Oracle Java 8 is preferred. For Ubuntu, you can follow this article http://tecadmin.net/install-oracle-java-8-jdk-8-ubuntu-via-ppa/, for other distribution, download from the Oracle website and install manually.
2. Scala Build Tool (SBT) is needed. Follow download section at the website to install http://www.scala-sbt.org/download.html
3. We use snapshot versions for Scorex and IODB. Please build and publish them locally because of that

IODB:

```
git clone https://github.com/input-output-hk/iodb.git
sbt publishLocal
```

Scorex:

```
git clone https://github.com/ScorexFoundation/Scorex.git
sbt publishLocal
```

1. Build and run TwinsChain

how much is needed to mess up our system?

The simulation results show that even with 70% of total mining power an adversary also needs for about 20% of total stake to generate abetter chain than honest party's.

Given Bitcoin capitalization of ~ $80 billion, 20% of stake is about $16 billion.

V.2

TwinsChain

[Chepurnoy,Duong,Fan,**Z**.,16]

- Scalable to a huge network of nodes
- provably secure
- adaptive difficulty adjustment
- implementation
- incentives
- Mode switching
- Stress test

Alternative Mechanisms

A Design Technique:
Constructing blockchains via blockchains

i-hop Blockchain

- **i=1, other than Bitcoin**
- **i=2,**
- **i=3,**
- **….**

References

- BitcoinNG; Hybrid consensus; Elastico; ByzCoin;

- 2-hop blockchain;

Alternative Mechanisms

Another Design Example: iChing

iChing:
scalable pure proof-of-stake blockchain in the open setting

The core-chain

$$\mathsf{H}(\mathsf{hash}(B_i), \mathtt{round}, \mathrm{PK}, \sigma) < \mathrm{T}$$

KEY POINT:

round is used;

digital signature is used.

Fan, Zhou, iChing: A scalable proof-of-stake blockchain in the open setting (or, How to Mimic Nakamoto's Design via Proof-of-Stake). IACR ePrint 2017

iChing:
scalable pure proof-of-stake blockchain
in the open setting

The core-chain

$$\mathsf{H}\left(\boxed{\text{hash}(B_i), \texttt{round}, \texttt{PK},}\ \sigma\right) < \mathrm{T}$$

Deterministic

Unique Signature

iChing: scalable pure proof-of-stake blockchain in the open setting

The core-chain

$$\mathsf{H}(\mathsf{hash}(B_i), \mathtt{round}, \textsc{pk}, \sigma) < \mathrm{T}$$

Assumptions:

- All the players are connected with bounded network delay.
- Majority of stake holders are honest.
- **The rate of block generation is low.**

SAME WITH POW BLOCKCHAIN !

iChing:
scalable pure proof-of-stake blockchain
in the open setting

The core-chain

$$\mathsf{H}(\mathsf{hash}(B_i), \mathtt{round}, \textsc{pk}, \sigma) < \mathrm{T}$$

Best chain strategy

- Longest chain is the best chain.
- The chain can be divergent from some block.
- **The view of best chain for different players will merge.**

SAME WITH POW BLOCKCHAIN !

iChing:
scalable pure proof-of-stake blockchain in the open setting

The core-chain

$$\mathsf{H}(\mathsf{hash}(B_i), \mathtt{round}, \text{PK}, \sigma) < \mathrm{T}$$

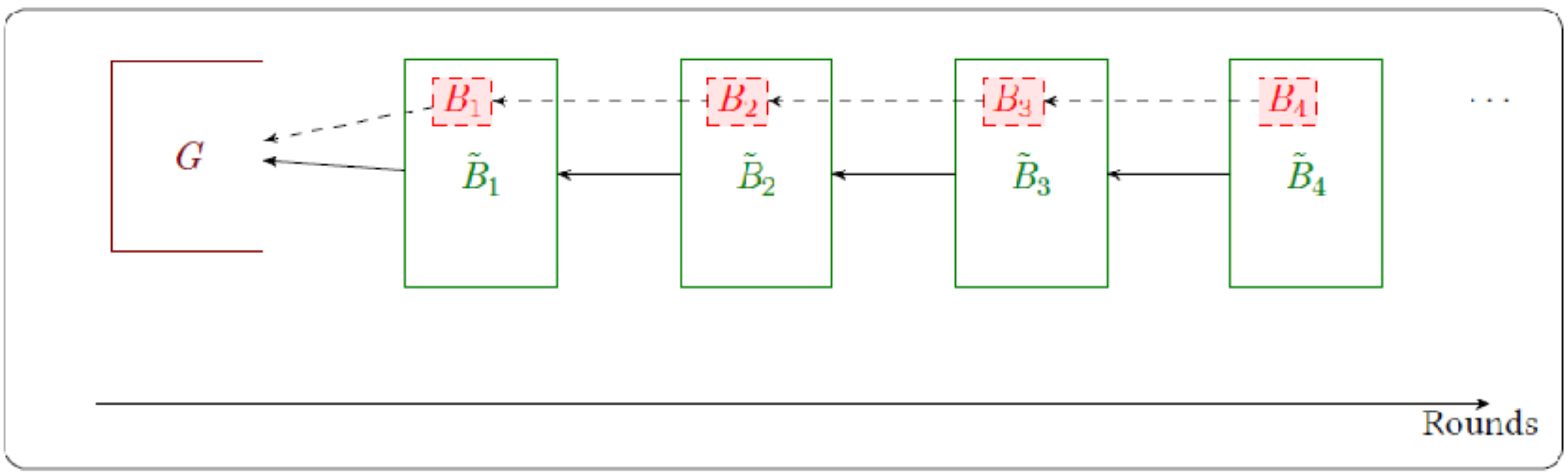
Why it works

- The honest stake holders will work on the same chain in most rounds.
- Every stake has the same probability to generate a block in a round.
- The honest best chain will grow faster than the others.
- No one can predict who can generate the block in a round.

iChing:
scalable pure proof-of-stake blockchain
in the open setting

From core-chain to blockchain

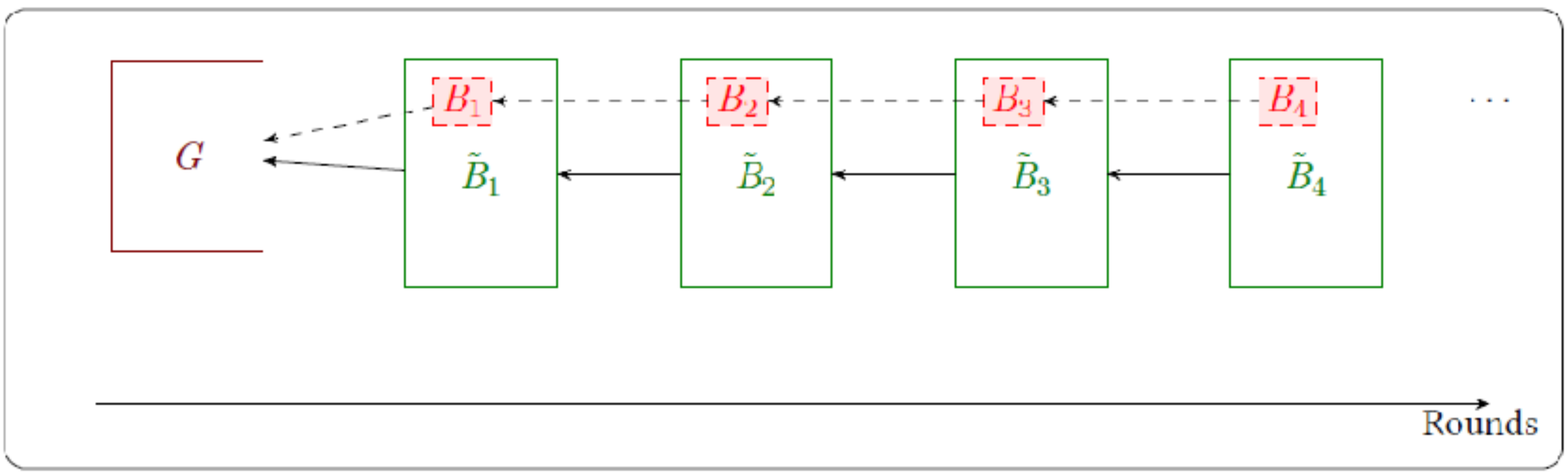
$$\tilde{B}_{i+1} = \langle \mathsf{hash}(\tilde{B}_i), B_{i+1}, \tilde{X}_{i+1}, \tilde{\mathrm{PK}}, \tilde{\sigma} \rangle$$



iChing:
scalable pure proof-of-stake blockchain
in the open setting

From core-chain to blockchain

$$\tilde{B}_{i+1} = \langle \mathsf{hash}(\tilde{B}_i), B_{i+1}, \tilde{X}_{i+1}, \tilde{\mathrm{PK}}, \tilde{\sigma} \rangle$$



the blockchain will not change the extension of the core-chain.

blocks in blockchain can be mapped to blocks in the core-chain, one by one.

the security of the blockchain can be reduced to the security of the core chain

Cryptography on the Blockchain

the sky is the limit !

Fair Multi-Party Computation

[Kiayias, **Z**, Zikas, 16]

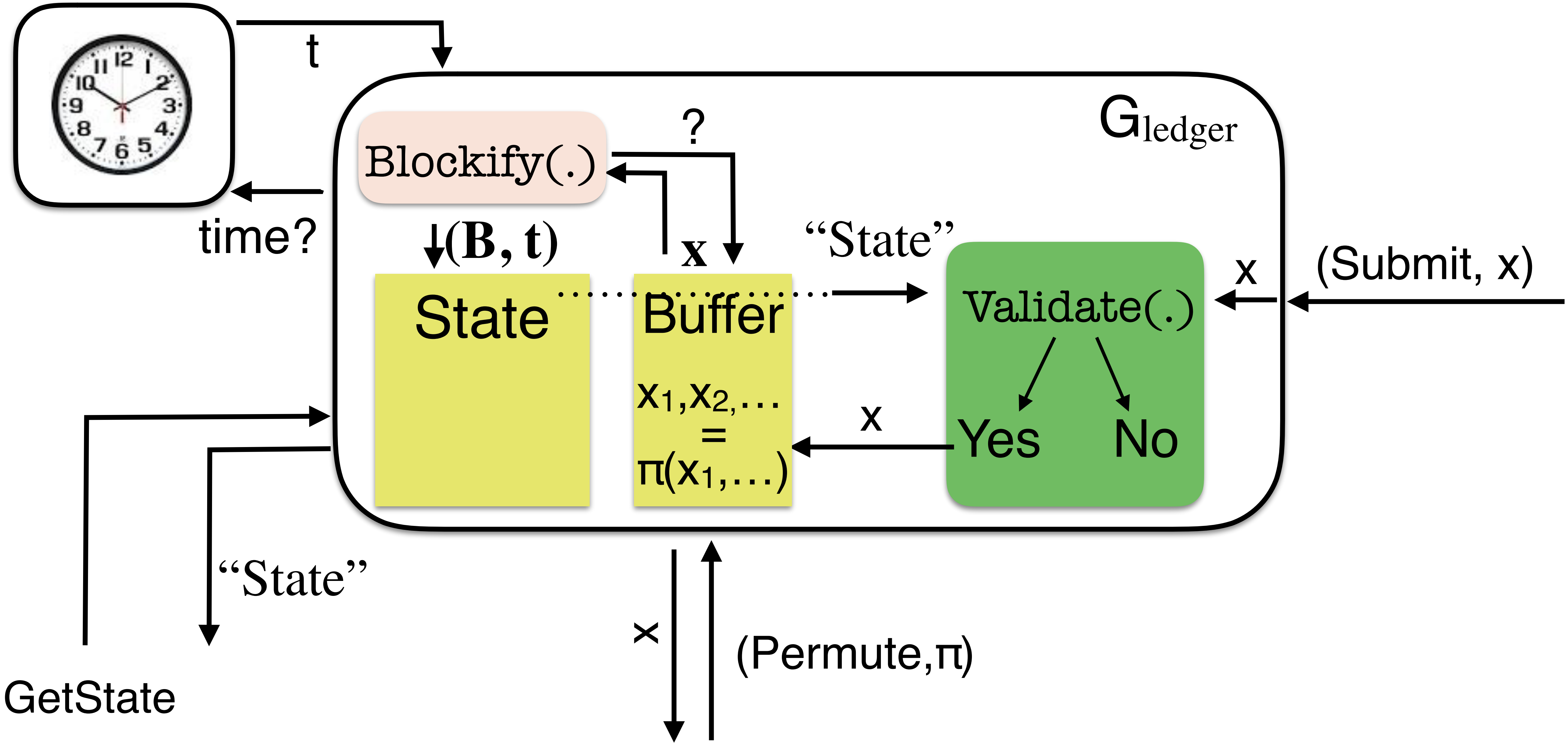
- fairness = honest users get compensated by the adversarial users when the protocol aborts in an unfair manner

- first result that achieves such fairness for multi-party computation via blockchain with Universal Composability

Kiayias, Zhou, Zikas, Fair and Robust Multi-Party Computation using a Global Transaction Ledger, Eurocrypt 2016

The Public Transaction Ledger & Time

[Kiayias, Z, Zikas, 16]

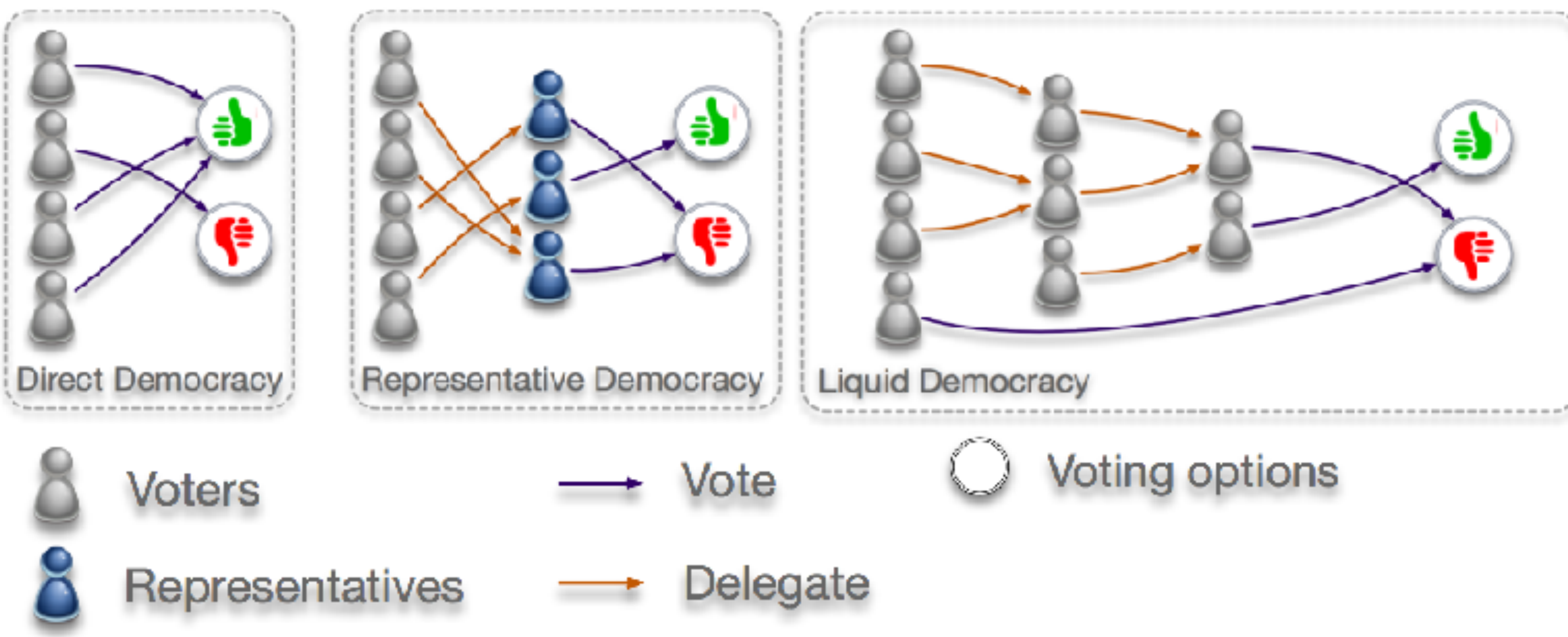


Can reorder **the recently inserted** transactions

Statement Voting

[Zhang, **Z**, 17]

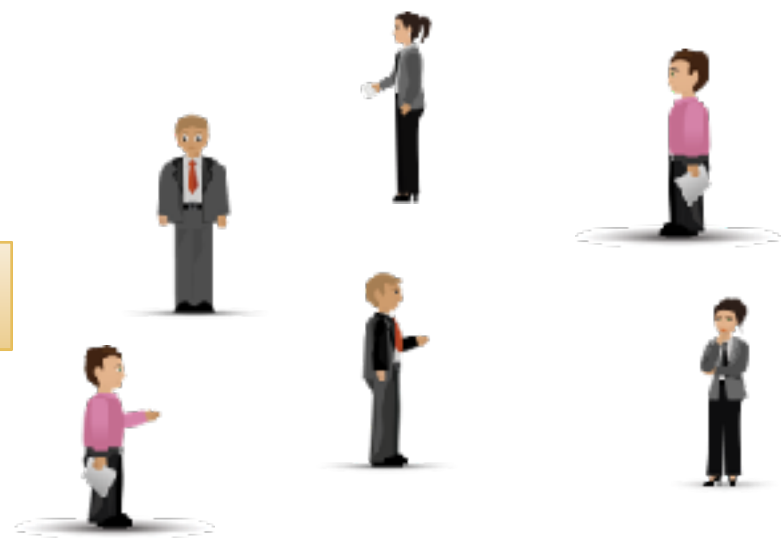
Liquid democracy (a.k.a. delegative democracy) [Ford 2002] is a hybrid of direct democracy and representative democracy, where the voters can either vote directly on issues, or they can delegate their votes to representatives who vote on their behalf.



Zhang, Zhou, Digital Liquid Democracy: How to Vote Your Delegation Statement, IACR ePrint 2017. PODC 2017, brief announcement.

statement voting: advantage

Voters



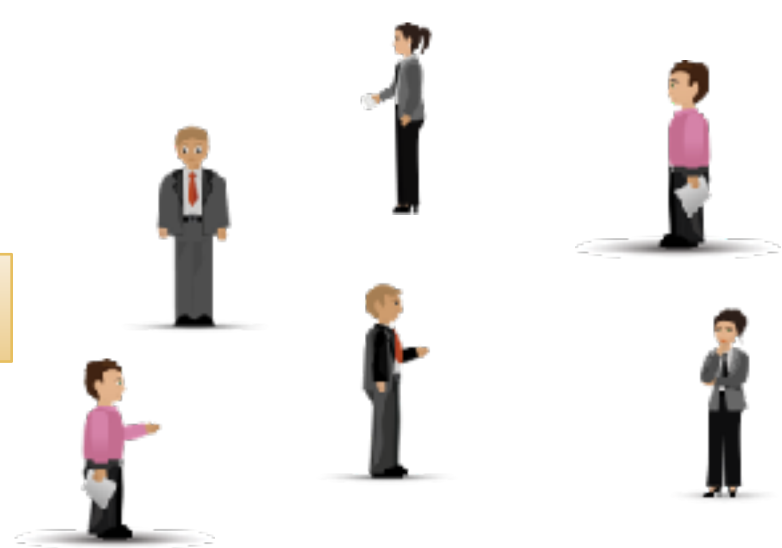
vote for candidate #1

vote for candidate #2

Determine the vote immediately in the voting phase

Determine the vote in the tally phase

Voters



P1 votes for candidate #1

P2 follows P1

P3 follows P1 if P1 votes; otherwise votes for candidate #2

statement voting — with privacy

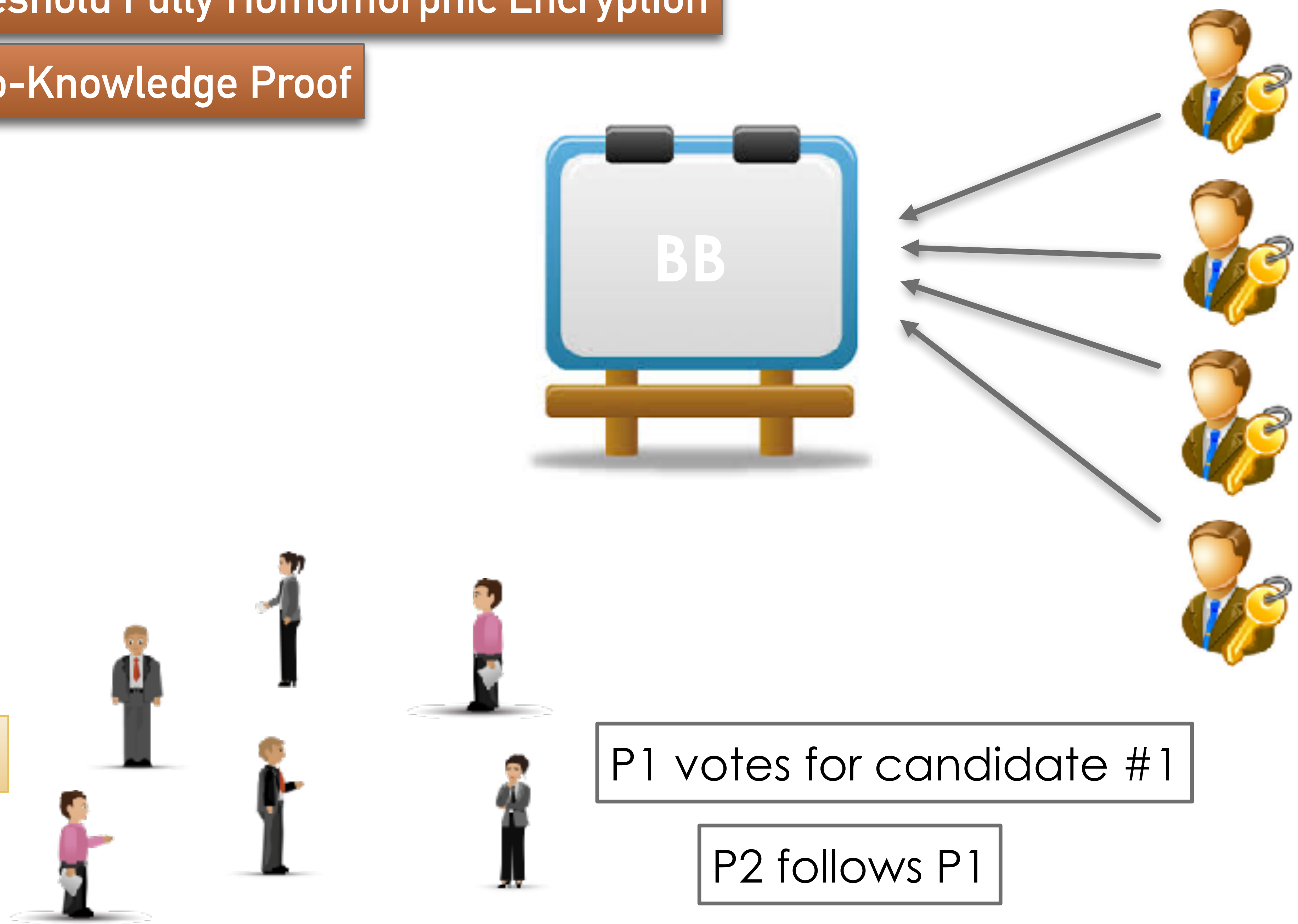
Helios*
not practical

tally circuit: process the voting statements

Trustees

Threshold Fully Homomorphic Encryption

Zero-Knowledge Proof



Voters

P1 votes for candidate #1

P2 follows P1

P3 follows P1 if P1 votes; otherwise votes for candidate #2

statement voting — with privacy

full version
practical

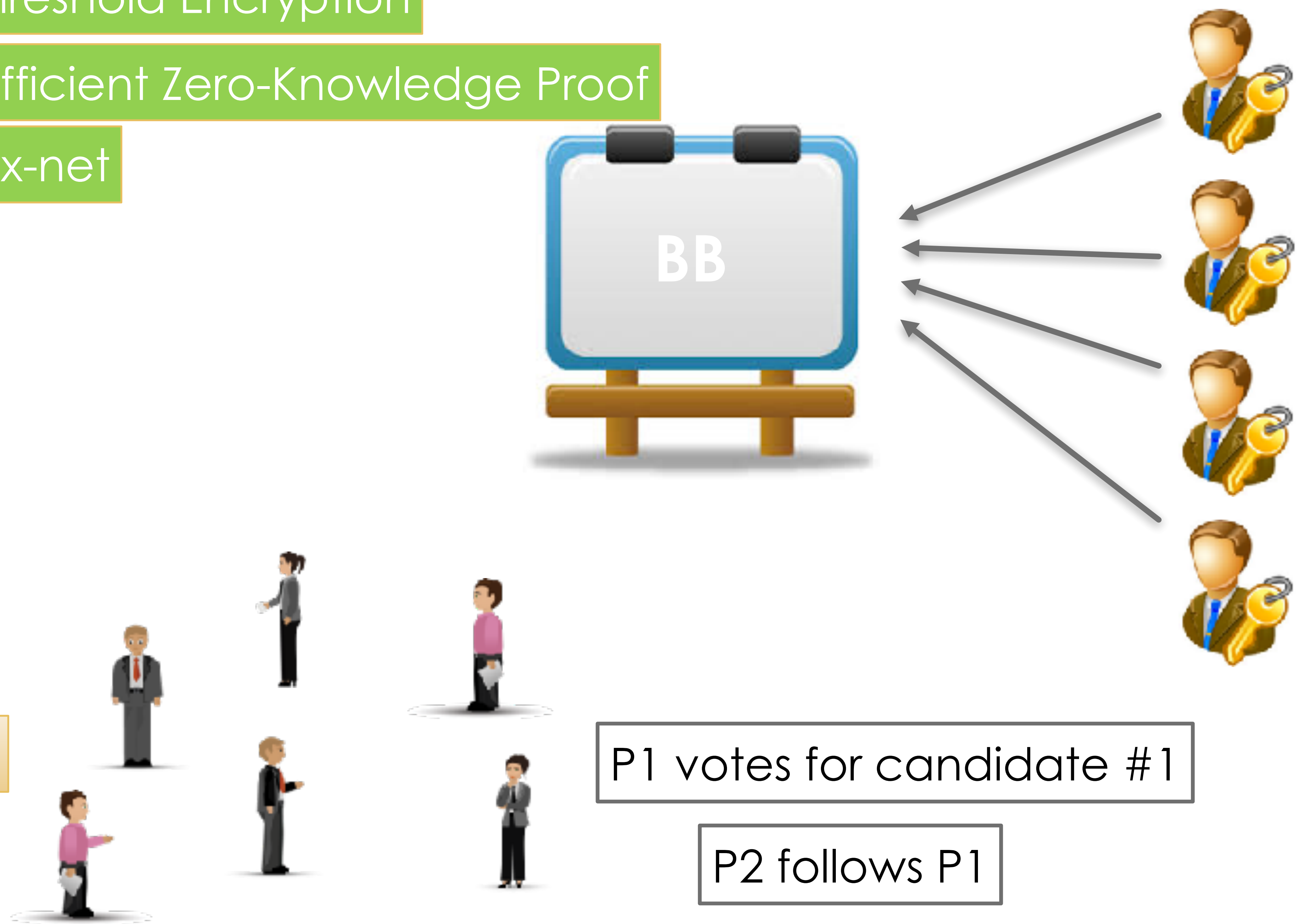
tally circuit: process the voting statements

Threshold Encryption

efficient Zero-Knowledge Proof

Mix-net

Trustees



Voters

P1 votes for candidate #1

P2 follows P1

P3 follows P1 if P1 votes; otherwise votes for candidate #2

my efforts along this line

Blockchain-based applications

- Zhang, Zhou, Digital Liquid Democracy: How to Vote Your Delegation Statement, IACR ePrint 2017. PODC 2017, brief announcement
- Kiayias, Zhou, Zikas, Fair and Robust Multi-Party Computation using a Global Transaction Ledger, Eurocrypt 2016

Consensus design and analysis

- Fan, Zhou, iChing: A scalable proof-of-stake blockchain in the open setting (or, How to Mimic Nakamoto's Design via Proof-of-Stake). IACR ePrint 2017
- Duong, Fan, Zhou, 2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely. IACR ePrint 2016
- Chepurnoy, Duong, Fan, Zhou, TwinsCoin: A Cryptocurrency via Proof-of-Work and Proof-of-Stake. IACR ePrint 2017
- Blocki, Zhou, Designing Proof of Human-work Puzzles for Cryptocurrency and Beyond. TCC 2016
- Duong, Zhou, Chepurnoy, Multi-Mode Cryptocurrency Systems. Manuscript.
- Katz, Garay, Kumaresan, Zhou, Adaptively Secure Broadcast, Revisited. PODC, 2011

https://cryptographylab.bitbucket.io/blockchain.html

Thanks

Cryptographic Foundations
of
Blockchains

Hong-Sheng Zhou
Virginia Commonwealth University
http://www.people.vcu.edu/~hszhou/
hongsheng.zhou@gmail.com