Introduction to Blockchain Security and Dependability Challenges -- A viewpoint

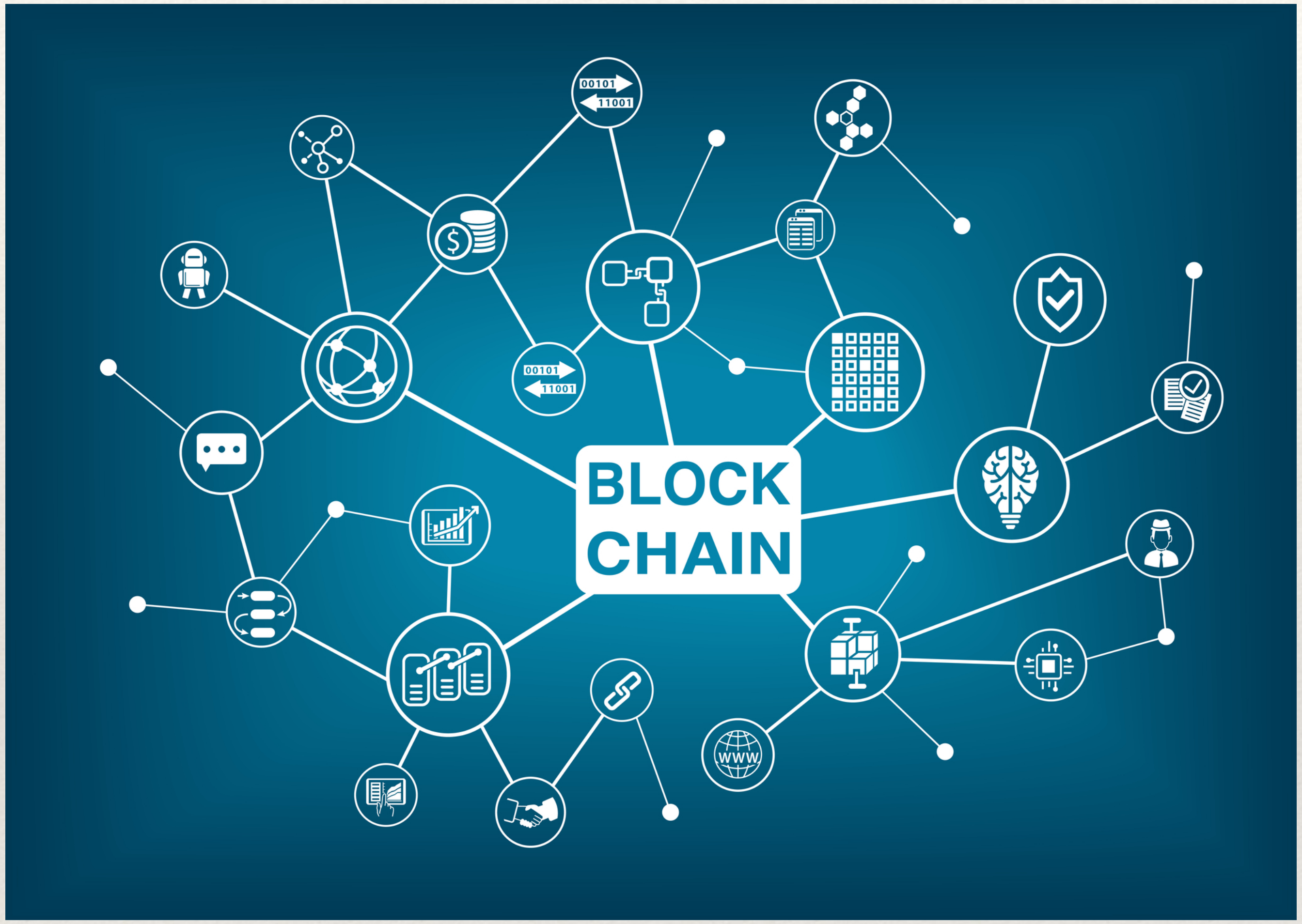
Jiangshan Yu
SnT - Interdisciplinary Centre for Security, Reliability and Trust
University of Luxembourg

June-2018

What is Blockchain?

A distributed database records all activities as transactions

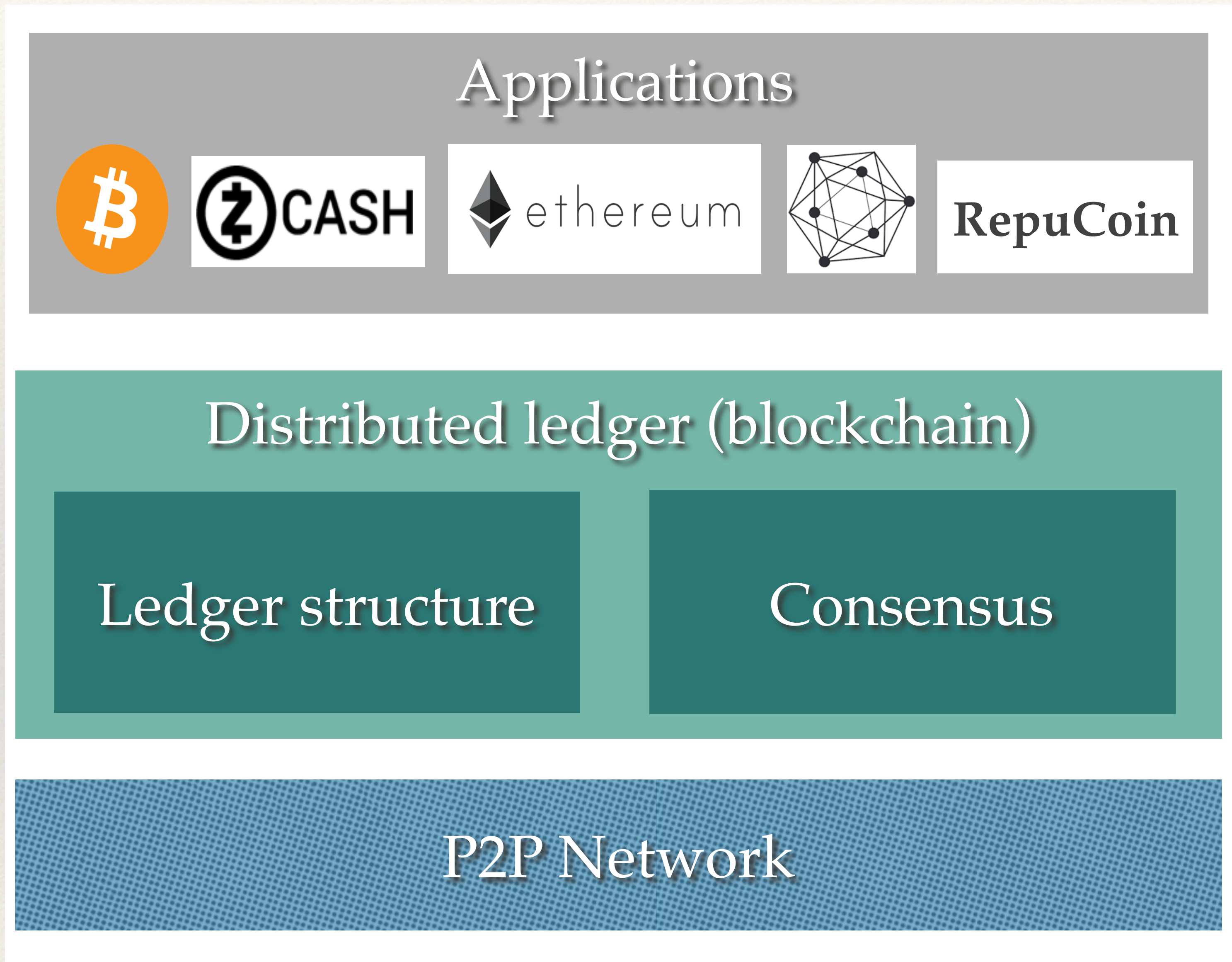
Why Blockchain?



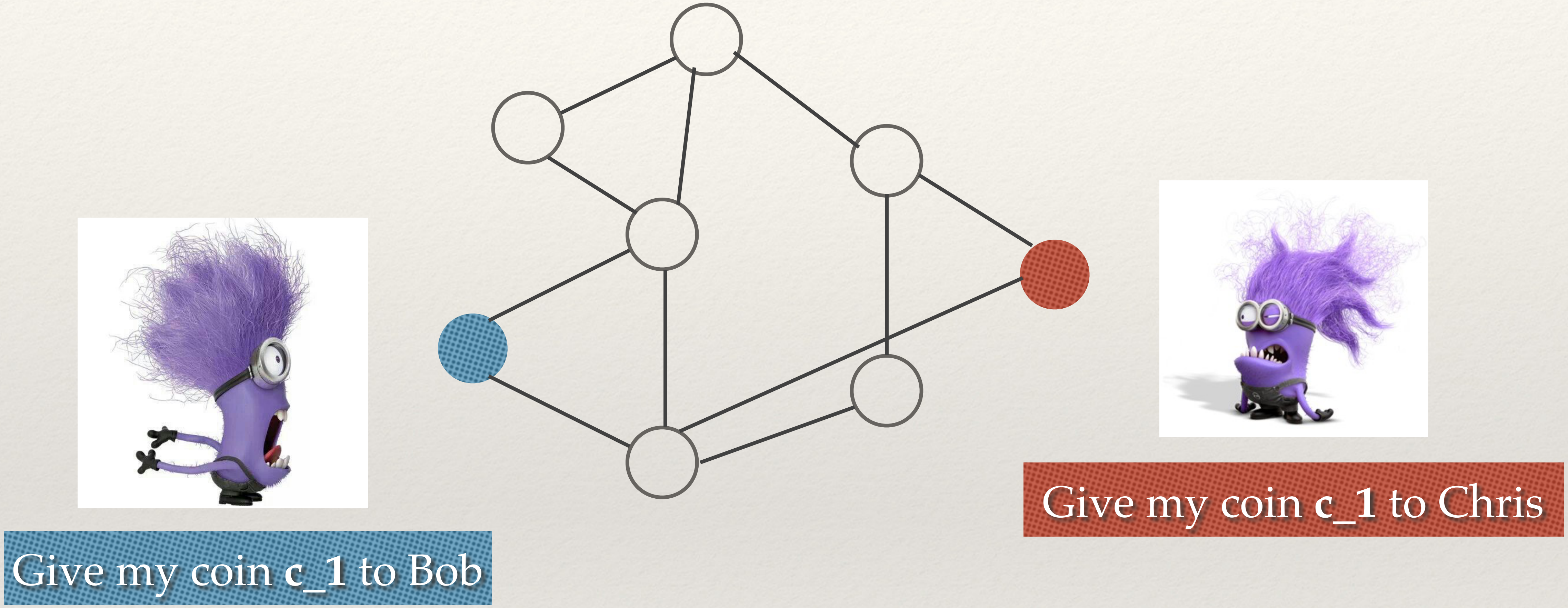
Goals:

- Secure: non-changeable history
- Robust: no single point of failure
- Transparent: everyone can read
- TTP free: everyone can write

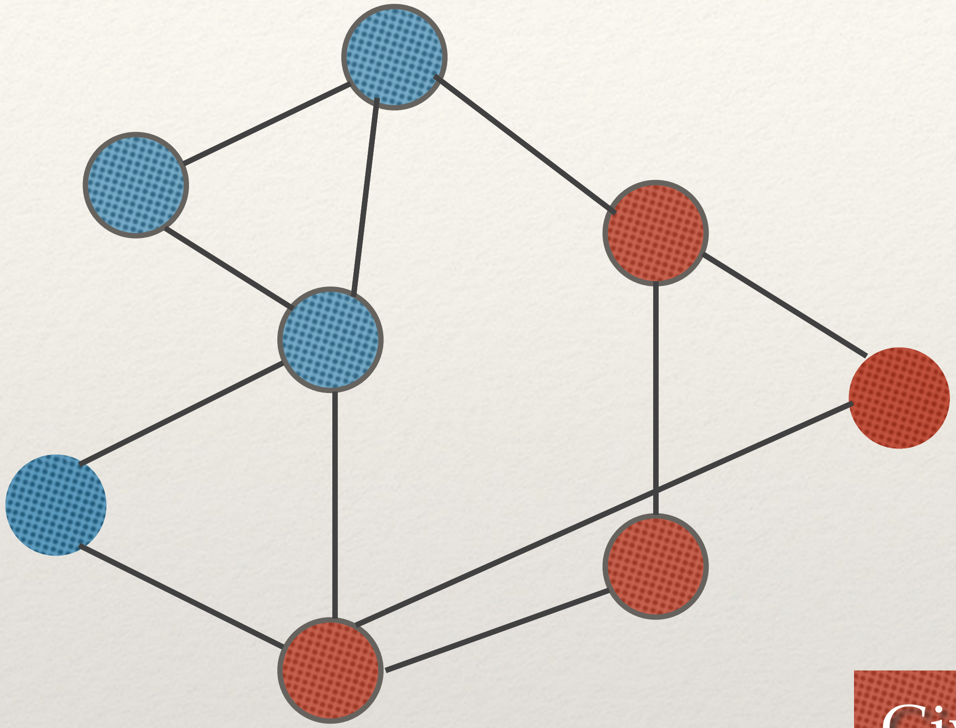
Architecture



Conflict transactions



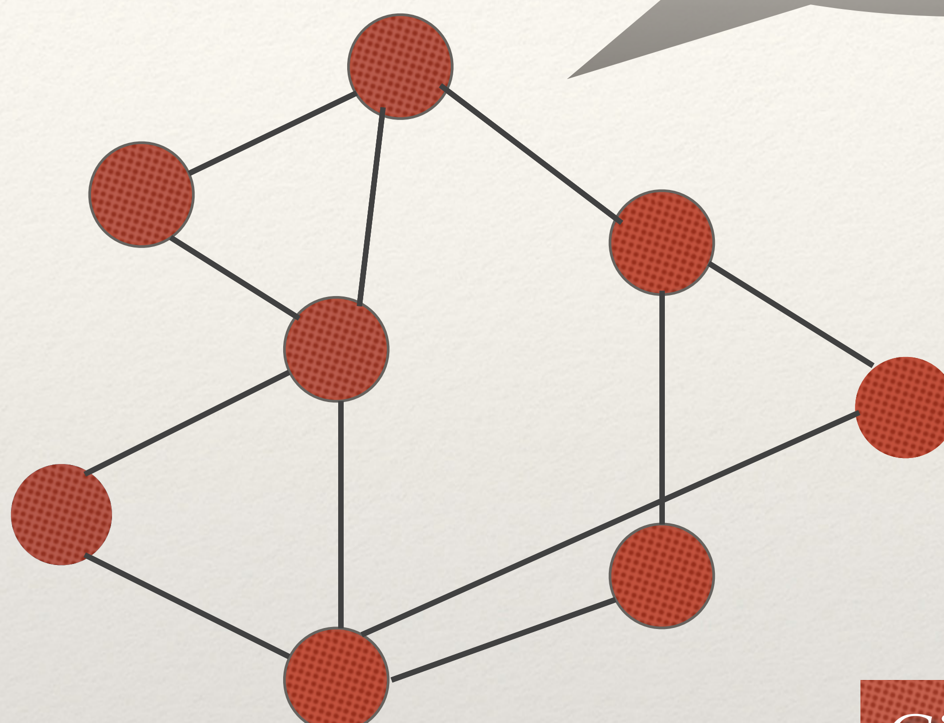
Conflict transactions



Give my coin **c_1** to Bob

Give my coin **c_1** to Chris

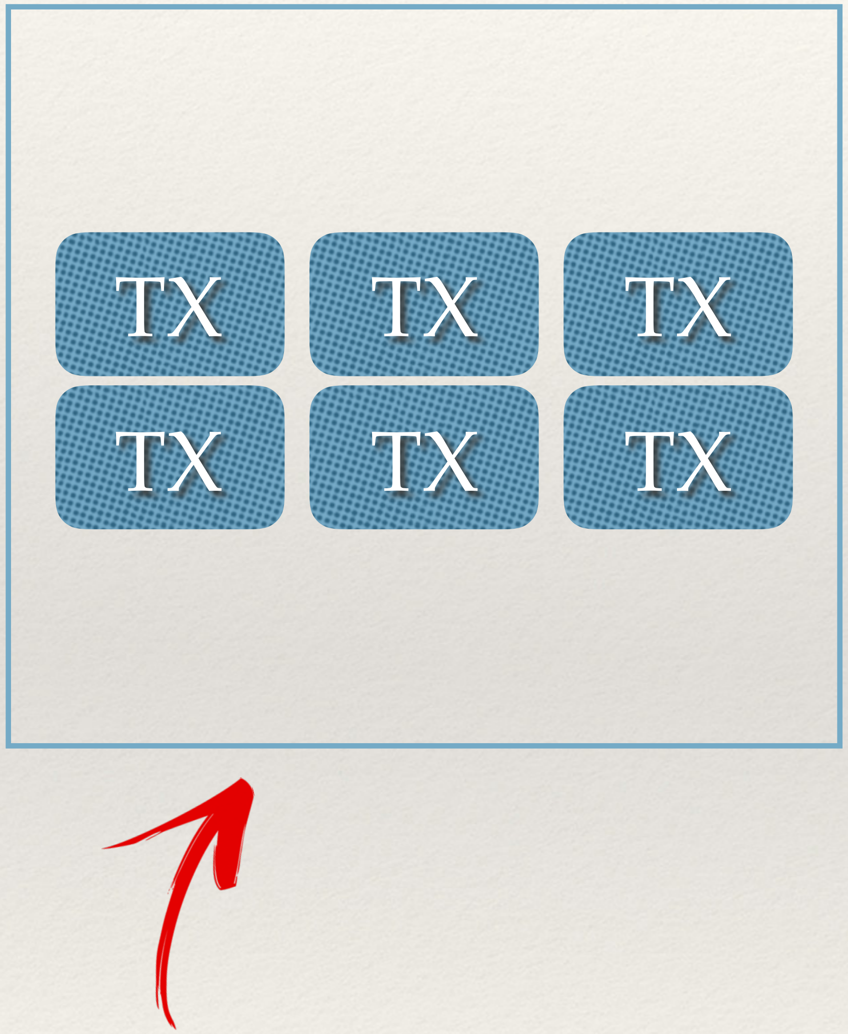
Conflict transactions



Give my coin **c_1** to Bob

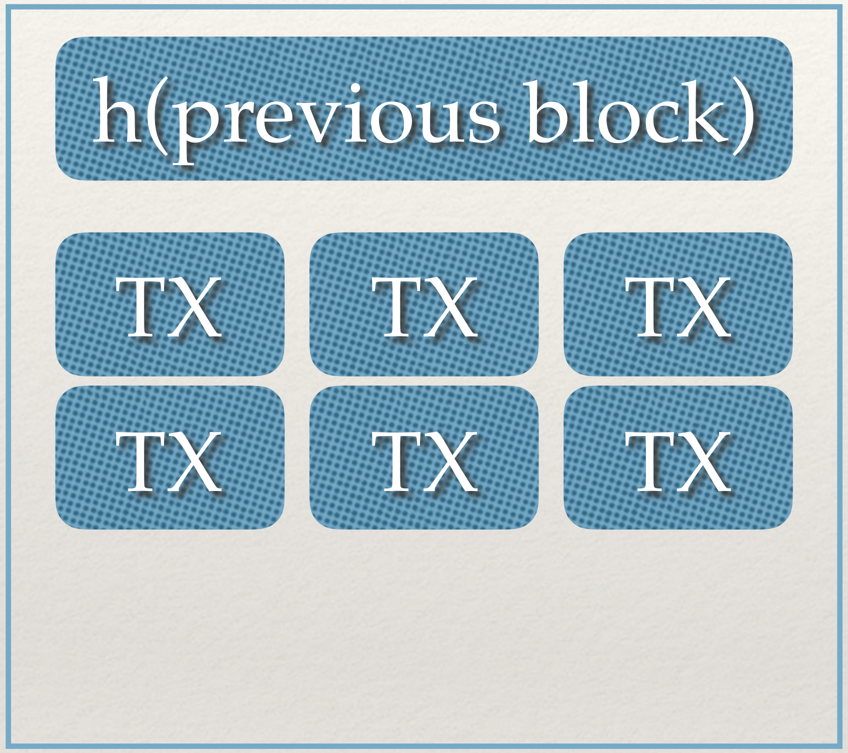
Give my coin **c_1** to Chris

Bitcoin: Proof of work



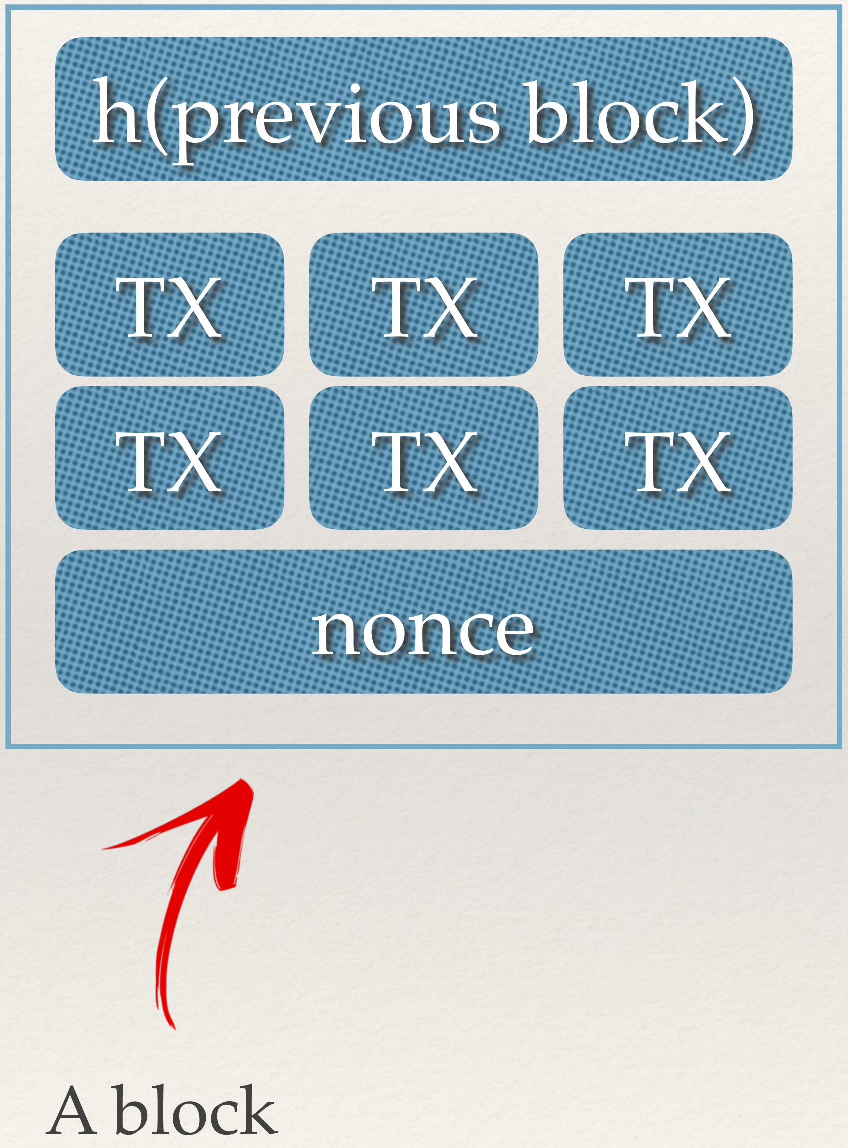
A block

Bitcoin: Proof of work



A block

Bitcoin: Proof of work

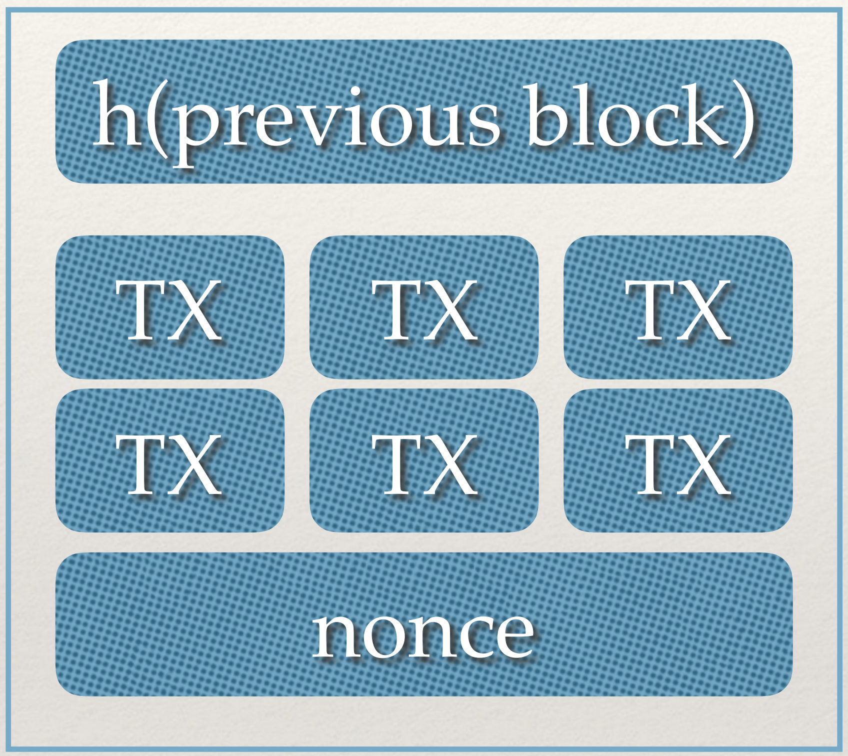


For nonce in $range(0, 2^{32})$:

```
if h(block) < target:
  print "success"
  break
else:
  continue
```

Bitcoin: Proof of work

SnT
securityandtrust.lu
CRITIX



A block

For nonce in $range(0, 2^{32})$:

```
if h(block) < target:
  print "success"
  break
else:
  continue
```

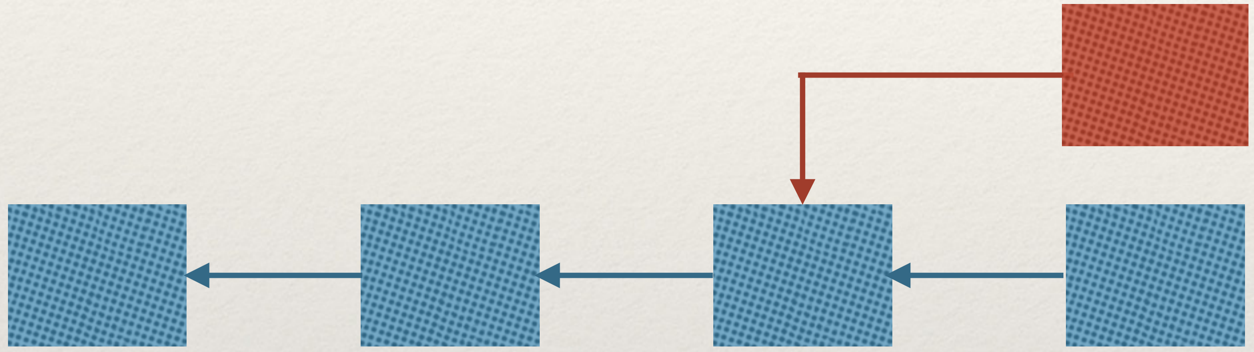
Problem A: **Slow TX validation**

10 mins/block, 7 transactions per second (TPS)

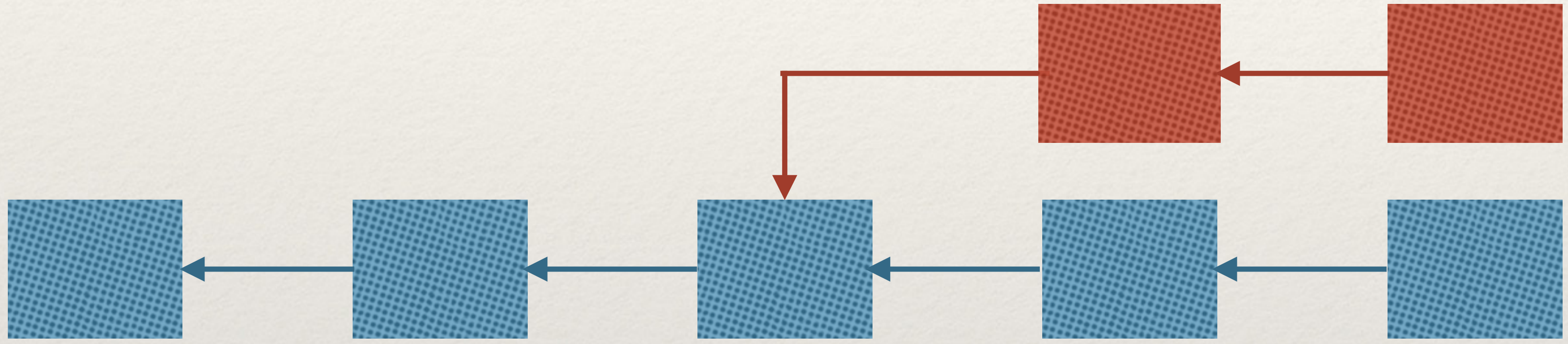
Problem B: **multiple valid solutions**

uni.lu UNIVERSITÉ DU LUXEMBOURG

Blockchain: resolving forks

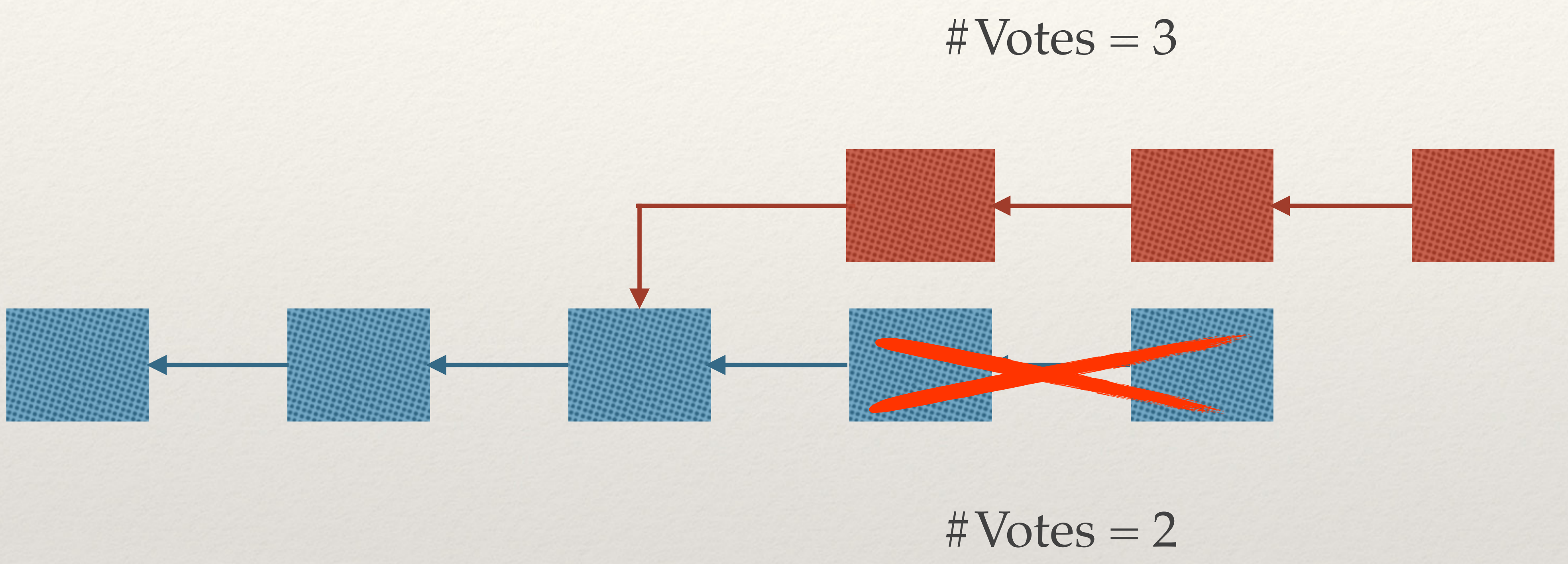


Blockchain: resolving forks



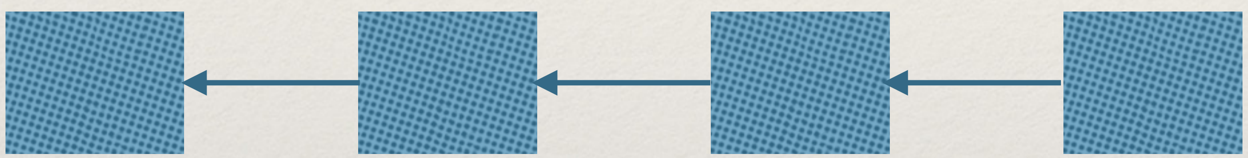
Blockchain: resolving forks

securityandtrust.lu
CRITIX



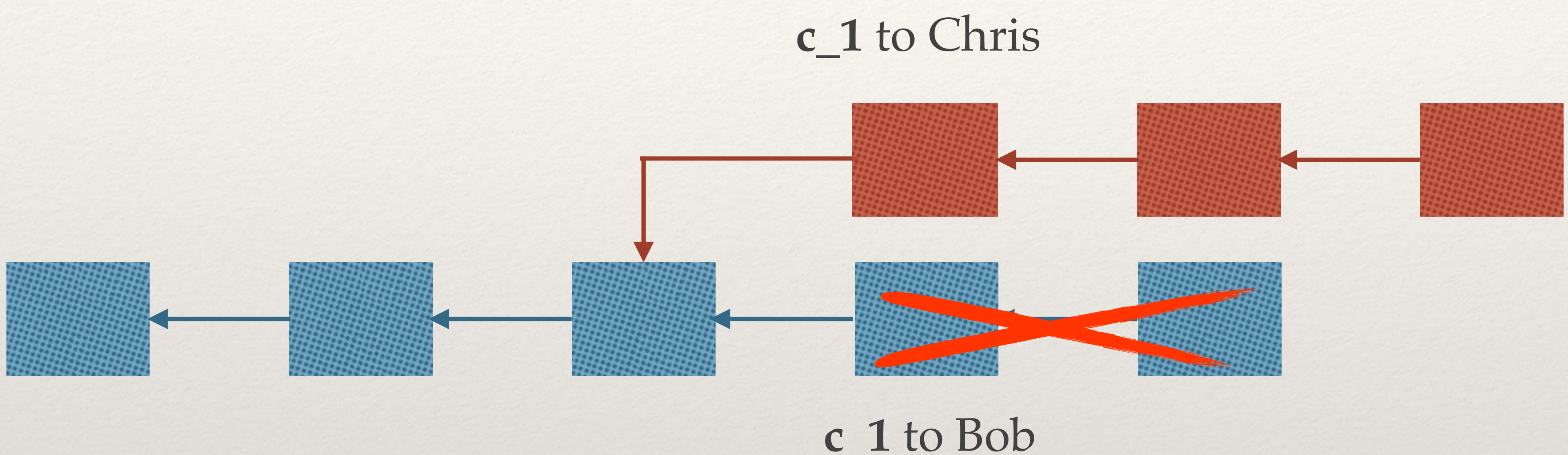
UNIVERSITÉ DU LUXEMBOURG

Double spending attack

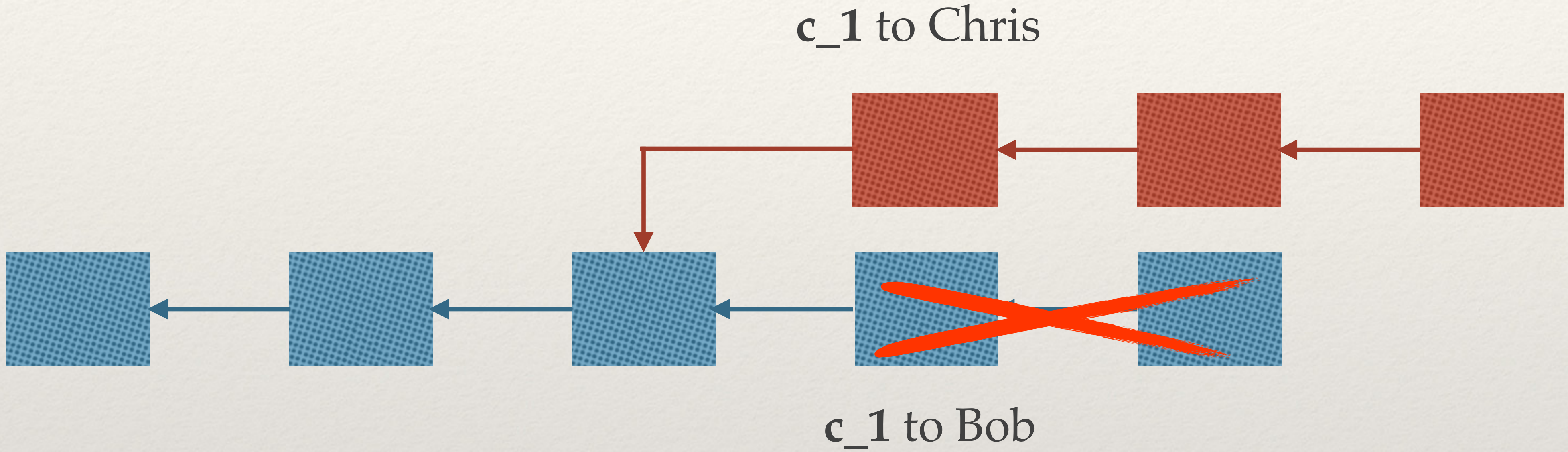


c_1 to Bob

Double spending attack



Double spending attack



If an attacker has >50% CPU power, it can spend a coin more than once.


51%
51% ATTACK
BITCOINS BIGGEST THREAT
www.newsbtc.com

Challenges

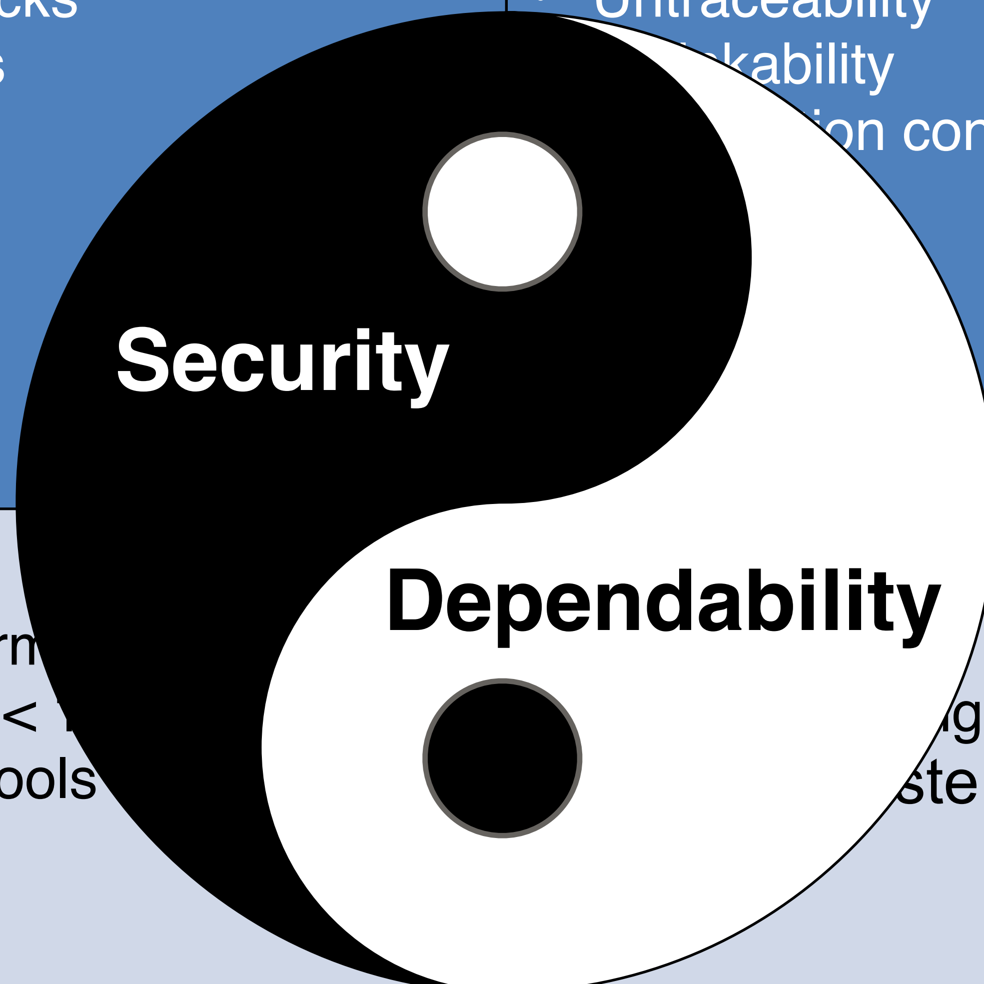
Security: • Double spending attacks • Selfish mining attacks • Flash attacks • Hijacking attacks • ...	**Privacy:** • Untraceability • Unlinkability • Transaction content privacy • …
Consensus: • Probabilistic v.s. deterministic • Limit fault quorums (f < 1/4? 1/3? 1/2?) • Oligopolistic mining pools - control • …	**Scalabilility:** • Limited #TPS • Ever increasing size of the ledger • Energy waste • …

Challenges

SnT
securityandtrust.lu
CRITIX

Security:
- Double spending attacks
- Selfish mining attacks
- Flash attacks
- Hijacking attacks
- ...

Privacy:
- Untraceability
- kability
- ion content privacy

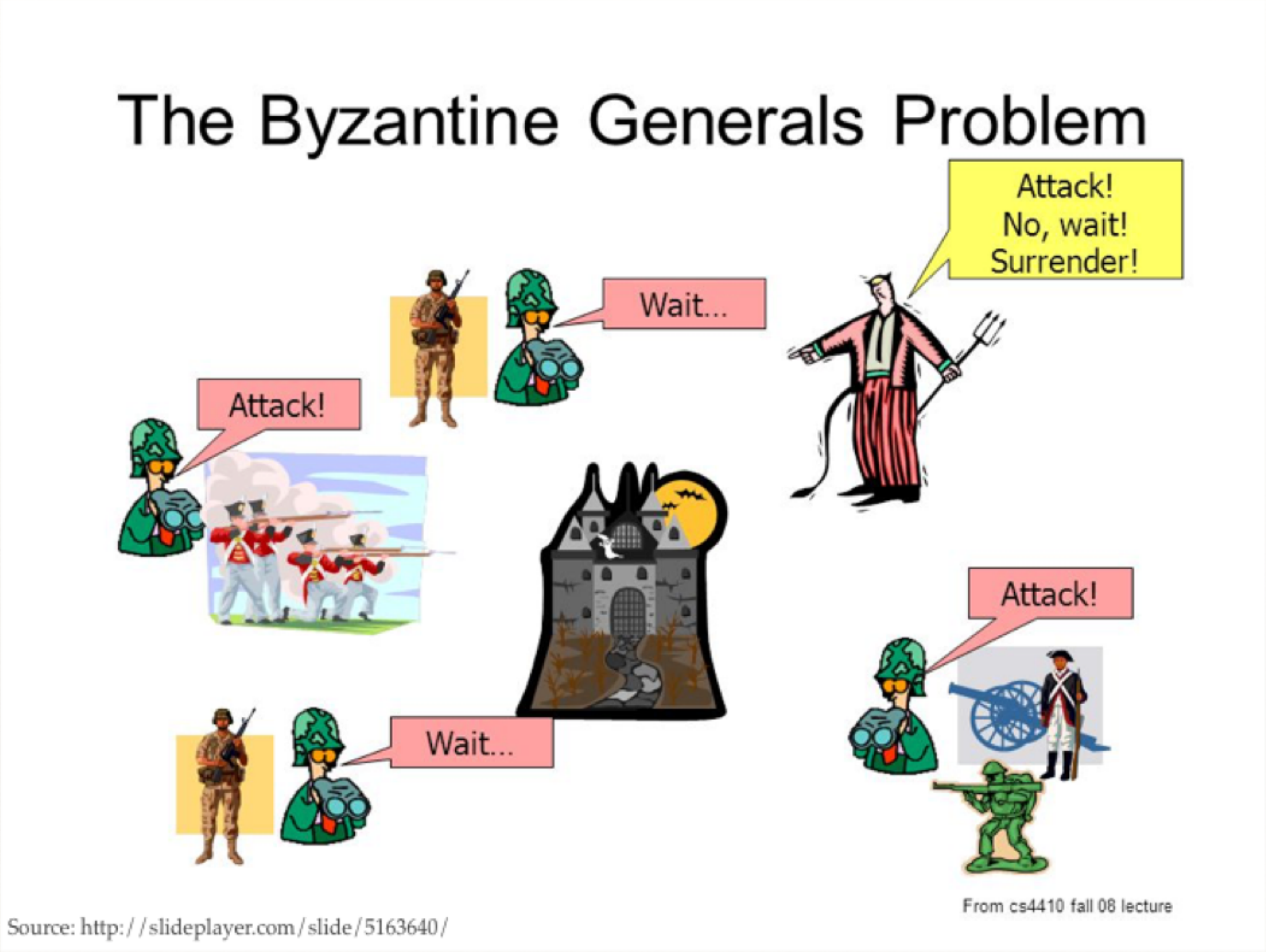


Consensus:
- Probabilistic v.s. determ
- Limit fault quorums (f < 1
- Oligopolistic mining pools
- …

g size of the ledger
ste

UNIVERSITÉ DU LUXEMBOURG

Dependability: 40 years of BFT research



Lamport, L.; Shostak, R.; Pease, M. (1982). "The Byzantine Generals Problem". ACM Trans. on Programming Languages and Systems. 4 (3): 382–401

Challenge 1: Mind the gap

SnT
securityandtrust.lu
CritiX

	BFT protocols	Permissionless Blockchain
Openess	A pre-fixed committee for voting	Open to everyone
Non-malicious participants	Honest	Honest or rational
Assumption	$f \leq \left\lfloor \frac{n-1}{3} \right\rfloor$	f < 50% mining power (BTC)
# voters	Small	Large
# players	N total; F faulty	?

uni.lu UNIVERSITÉ DU LUXEMBOURG

Applying BFT to Blockchain

Permissioned (consortium) Blockchain

A good start, but not the end…

BFT and Permissionless Blockchain

Challenge for system deployment:

How to define N? And hence predict F?

- *N is dynamic and can become very large*
- *In practice, in an open BFT-based system, we cannot guarantee that an attacker will not control more than a priori defined F nodes*

BFT and Permissionless Blockchain

SnT
securityandtrust.lu
CRITIX

Several prior efforts on applying BFT to Blockchain

- PeerCensus
- ByzCoin
- Solida
- Hybrid consensus
- Thunderella
- …

uni.lu
UNIVERSITÉ DU LUXEMBOURG

PoW+BFT

SnT securityandtrust.lu CritiX

- Setp 1. Run PoW to select a small number of members;
- Setp 2. Run BFT to reach agreement

N could be fixed and small this way

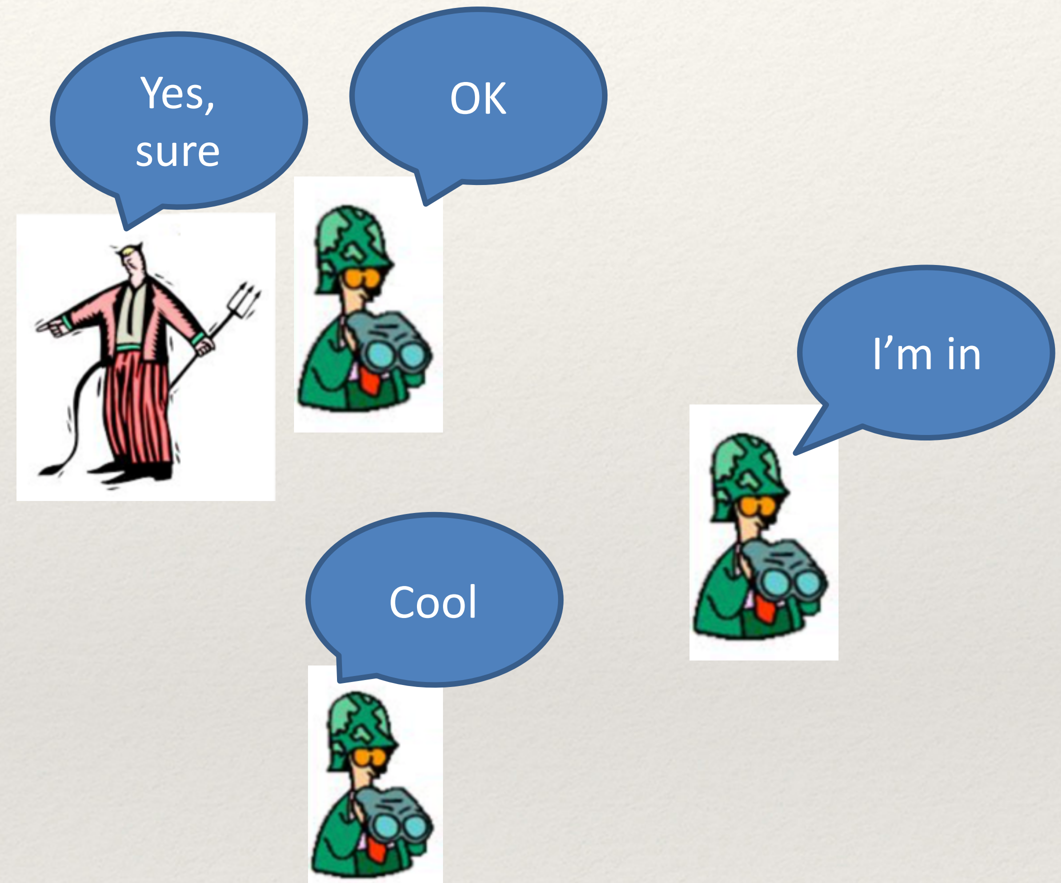
So, we could predict F …

… *Could we?* ...

UNIVERSITÉ DU LUXEMBOURG

Assumption v.s. Reality

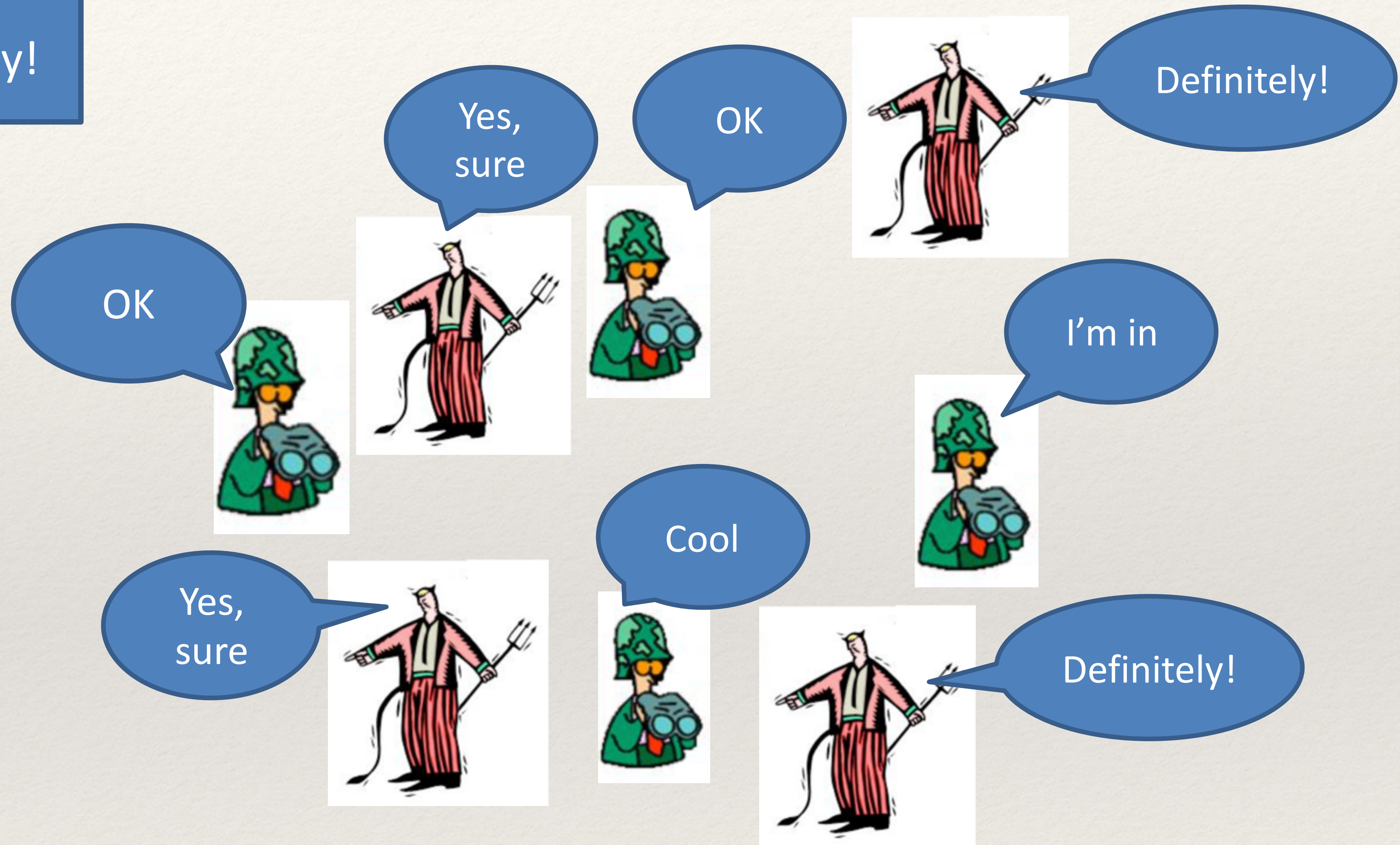
Byzantine generals plan!



Reality is….
If anyone can be selected to run consensus,
how can we be sure that the system contains no more than f malicious nodes?

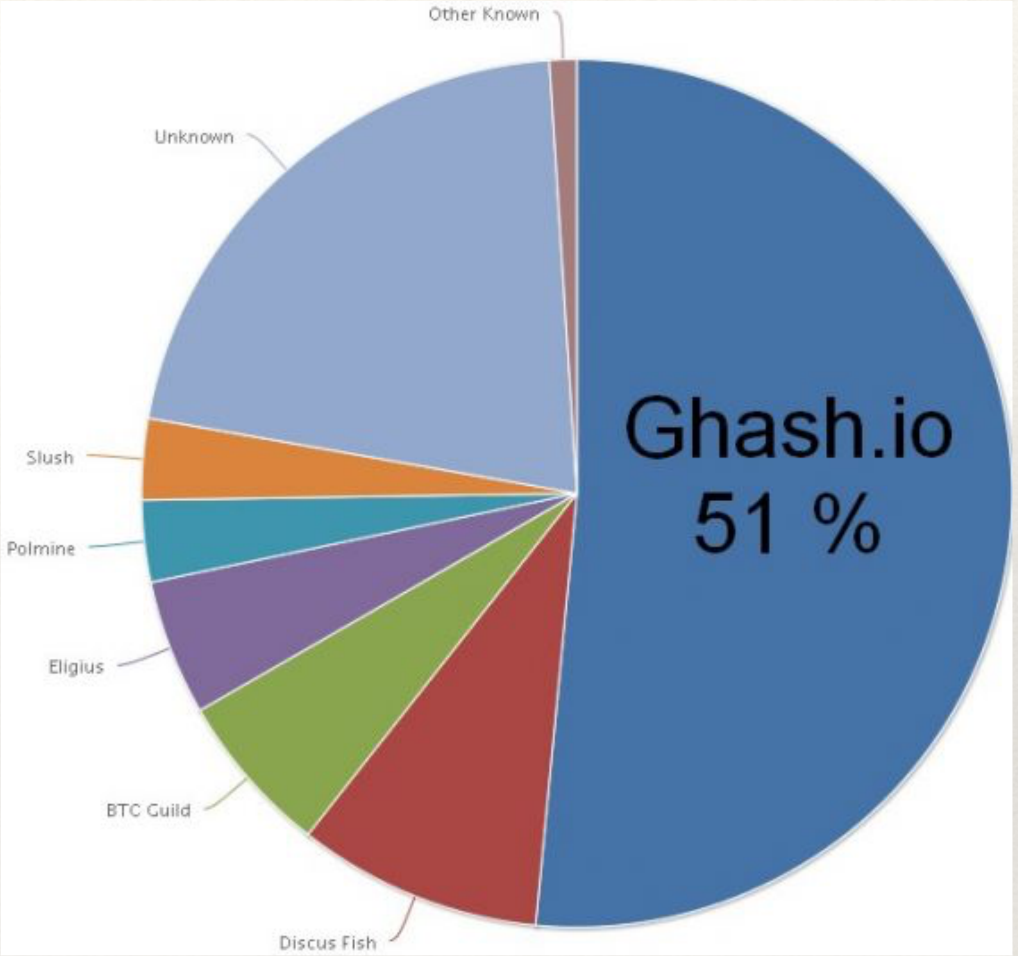
Assumption v.s. Reality

Byzantine generals plan!



Reality is….
If anyone can be selected to run consensus,
how can we be sure that the system contains no more than f malicious nodes?

Reality is tough



Reality is tough

2013

Majority is not Enough: Bitcoin Mining is Vulnerable*

Ittay Eyal and Emin Gün Sirer

Department of Computer Science, Cornell University
ittay.eyal@cornell.edu, egs@systems.cs.cornell.edu

Abstract. The Bitcoin cry **> 25%** rds its transactions in a public log called the blockchain. s critically on the distributed protocol that maintains the blockchain, run by participants called miners. Conventional wisdom asserts that the mining protocol is incentive-compatible and secure against colluding minority groups, that is, it incentivizes miners to follow the protocol as prescribed.
We show that the Bitcoin mining protocol is not incentive-compatible. We present an attack with which colluding miners obtain a revenue larger than their fair share. This attack can have significant consequences for Bitcoin: Rational miners will prefer to join the selfish miners, and the colluding group will increase in size until it becomes a majority. At this point, the Bitcoin system ceases to be a decentralized currency.

Reality is tough

2016

Why buy when you can rent?
Bribery attacks on Bitcoin-style consensus

Joseph Bonneau

Stanford University & Electronic Frontier Foundation

Abstract. The Bitcoin cryptocurrency introduced a novel distributed consensus mechanism relying on economic incentives. While a coalition controlling a majority of computational power may undermine the system, for example by double-spending funds, it is often assumed it would be incentivized not to attack to protect its long-term stake in the health

>50% CPU power for a short time.
(flash attack)

All existing PoW-based systems are vulnerable to this attack.

public, distributed ledger called the blockchain which logs all transactions to ensure that funds may only be spent once. Bitcoin uses a computational puzzle

Reality is tough

Attacks/Features	BitCoin	BitCoin-NG	ByzCoin
Double spending attacks	☠	☠	👌
Selfish mining attack	☠	☠	☠
Bribery/flash attack	☠	☠	☠
Eclipse attacks	☠	☠	😐
Non-forkable chain	☠	☠	👌
Liveness	👌	👌	☠
Throughput	7 tps	?	1,000 tps

👌 The system is secure against this attack

☠ The system is vulnerable to this attack

😐 The system can prevent double spending, but its throughput maybe reduced.

The big big challenge

SnT
securityandtrust.lu
CritiX

In a permissionless blockchain, how to enforce, at least with a very high probability, that

malicious_nodes $\leq$ F?

ΣP malicious_nodes $\leq P_F$?

UNIVERSITÉ DU LUXEMBOURG

Our solution: RepuCoin

SnT
securityandtrust.lu
CRITIX

The increase of any miner's voting power is bounded by "physics"!

$$\frac{dPd}{dN \cdot dt} = \frac{1}{2}\frac{\lambda}{(\lambda + |x-a|)^2} \leq \frac{1}{2\lambda}$$

λ and a are system parameters, and x is defined in the reputation algorithm.

uni.lu UNIVERSITÉ DU LUXEMBOURG

J.Yu,D.Kozhaya,J.Decouchant,and P.Esteves-Verissimo,"Repucoin: Your reputation is your power," Cryptology ePrint Archive, Report 2018/239, 2018, https://eprint.iacr.org/2018/239.

Comparison

Attacks/Features	BitCoin	BitCoin-NG	ByzCoin	RepuCoin
Double spending attacks	☠️	☠️	👌	👌
Selfish mining attack	☠️	☠️	☠️	👌
Bribery/flash attack	☠️	☠️	☠️	👌
Eclipse attacks	☠️	☠️	😐	😐
Non-forkable chain	☠️	☠️	👌	👌
Liveness	👌	👌	☠️	👌
Throughput	7 tps	?	1,000 tps	10,000 tps

👌 The system is secure against this attack

☠️ The system is vulnerable to this attack

😐 The system can prevent double spending, but its throughput maybe reduced.

Security and Dependability:

securityandtrust.lu

CRITIX

The minimum cost of successfully attacking RepuCoin

Joining time\ Target	1 week	1 month	3 months	6 months
1 month	infeasible	45%	30%	27%
3 months	infeasible	90%	45%	33%
6 months	infeasible	infeasible	68%	45%
9 months	infeasible	infeasible	90%	54%
12 months	infeasible	infeasible	infeasible	68%
18 months	infeasible	infeasible	infeasible	91%
20 months	infeasible	infeasible	infeasible	infeasible

UNIVERSITÉ DU LUXEMBOURG

The minimum cost of successfully attacking RepuCoin

Joining time\ Target	1 week	1 month	3 months	6 months
1 month	infeasible	BTC: *635; BYZ: *6	BTC: *1271; BYZ: *11	BTC: *2287; BYZ: *20
3 months	infeasible	BTC: *1270; BYZ: *11	BTC: *1906; BYZ: *17	BTC: *2795; BYZ: *25
6 months	infeasible	infeasible	BTC: *2880; BYZ: *26	BTC: *3812; BYZ: *34
9 months	infeasible	infeasible	BTC: *3812; BYZ: *34	BTC: *4574; BYZ: *41
12 months	infeasible	infeasible	infeasible	BTC: *5760; BYZ: *51
18 months	infeasible	infeasible	infeasible	BTC: *7708; BYZ: *69
20 months	infeasible	infeasible	infeasible	infeasible

How RepuCoin works?

securityandtrust.lu

I'LL BE BACK SOON!

@Sunday

Research Reports

Challenge 2: explosion of proposals

Proof of Stake,
PeerCensus,
Proof of Capacity,
Proof of Activity,
Proof of Deposit
Proof of Lock
Proof of Luck
Proof of Elapsed time
Proof of Space
Proof of Retrievability
Proof of Reputation,
Algorand
Ouroborus

Thunderella
Solida
ByzCoin
HoneyBadger
Ghost
Fruitchains
RedBelly
IoTA
....

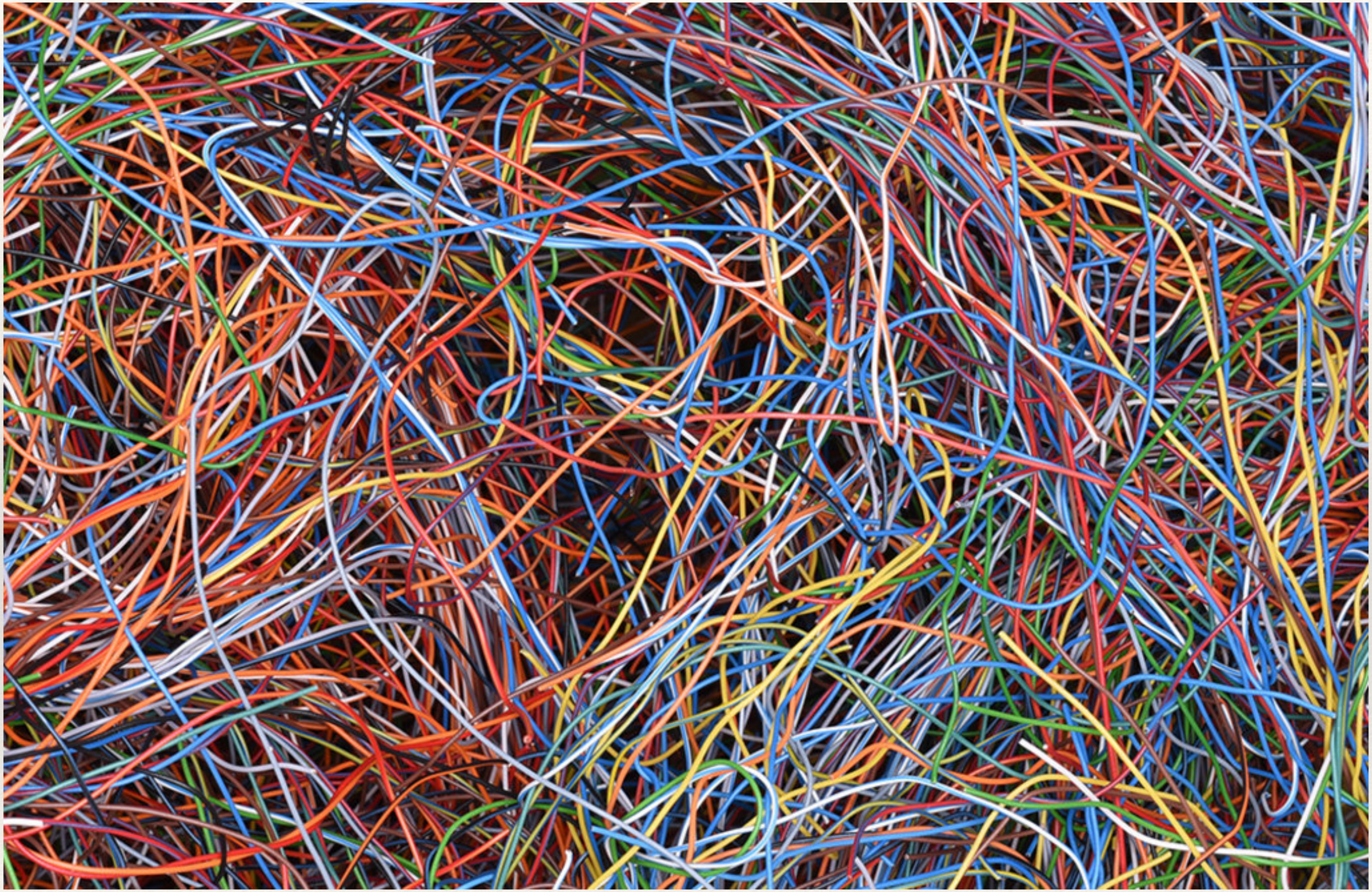
A lot of new proposals!

SnT securityandtrust.lu CRITIX

- Informal description (badly written white papers)
- Lack of formal models, e.g. system models and threat models
- No metrics to evaluate existing systems
- Heuristic analysis

A lot of new proposals!

SnT
securityandtrust.lu
CritiX



UNIVERSITÉ DU LUXEMBOURG

Our work:

Linking the Blocks: A Survey of Blockchain Consensus, 2018.

*Joint work (in progress) with Christopher Natoli, Vincent Gramoli, and Paulo Verissimo, 2018.

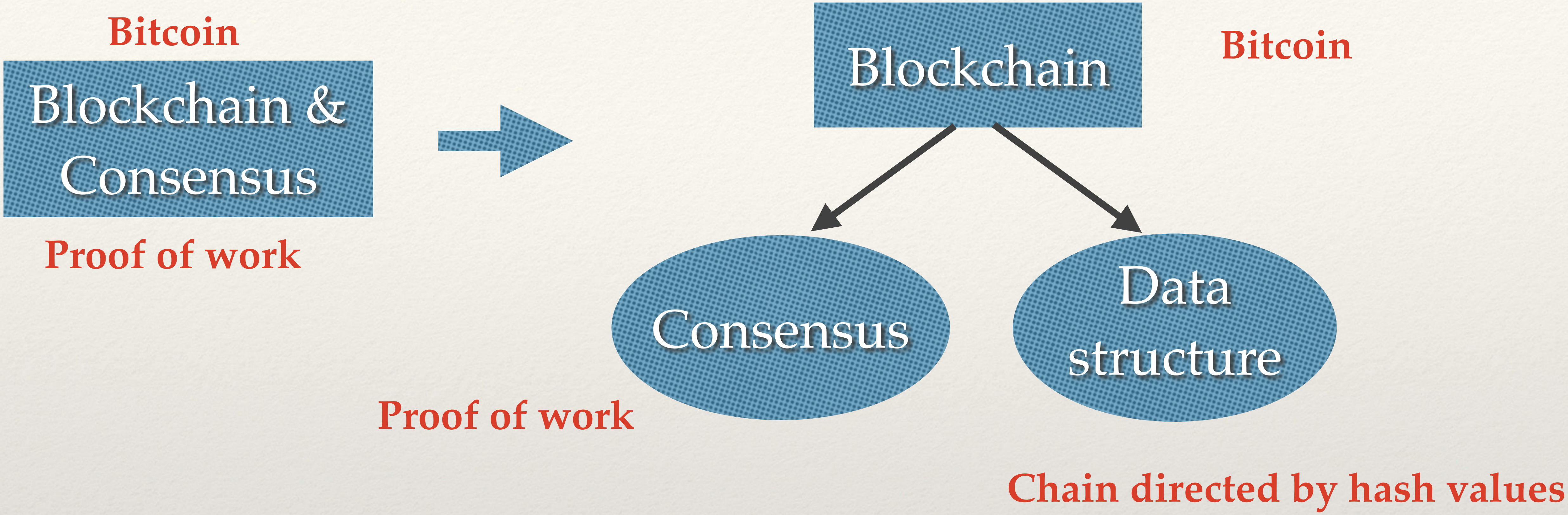
A new blockchain layer structure:

Bitcoin

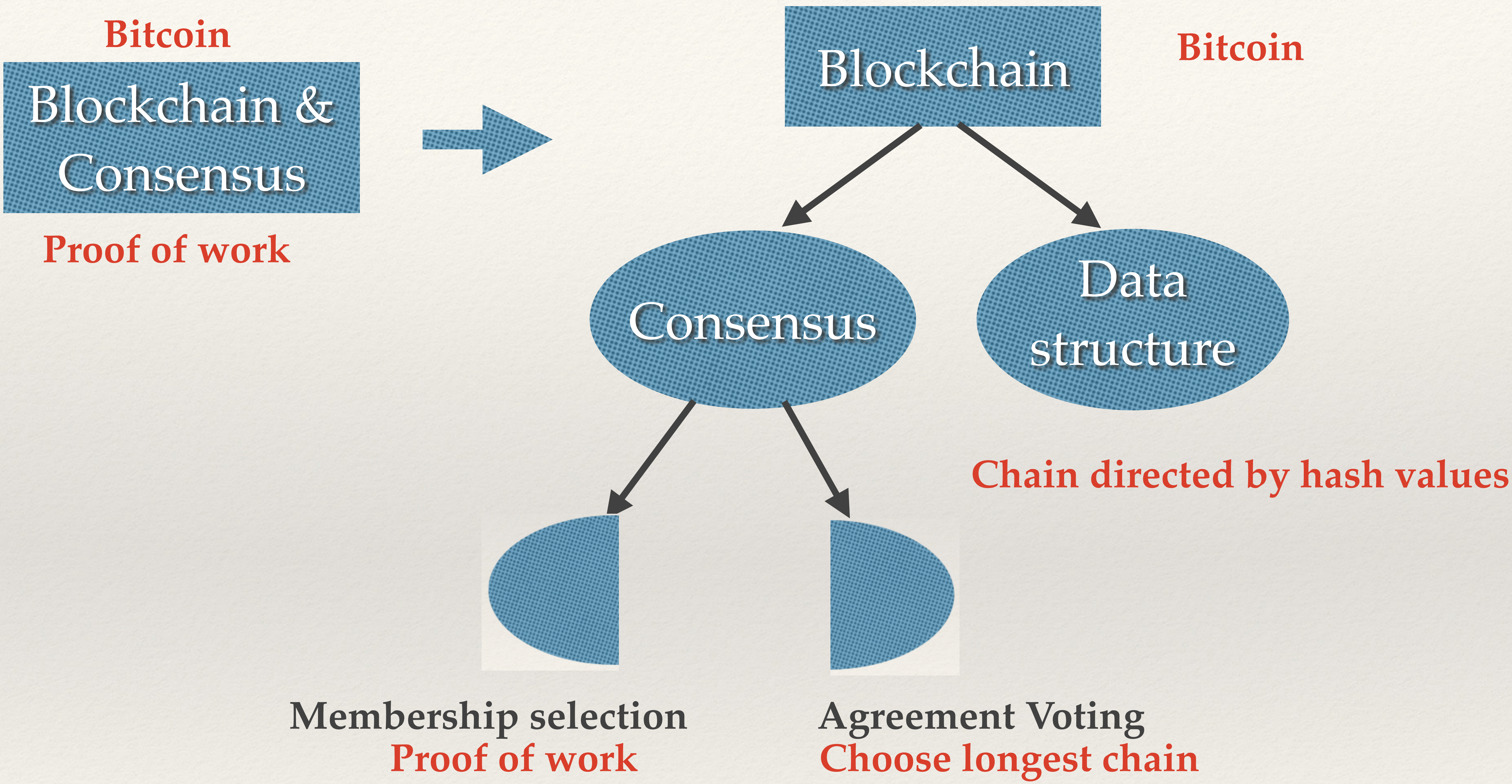
Blockchain & Consensus

Proof of work

A new blockchain layer structure:



A new blockchain layer structure:



Challenge 3: Privacy

Challenge: Reconcile Privacy and Transparency

Crypto-techniques

securityandtrust.lu

CRITIX

Deployed techniques:

1. Zero knowledge proof of knowledge
   (e.g. Zk-SNARKs in ZCash)
2. Linkable ring signature
   (e.g. RingCT in Monero)

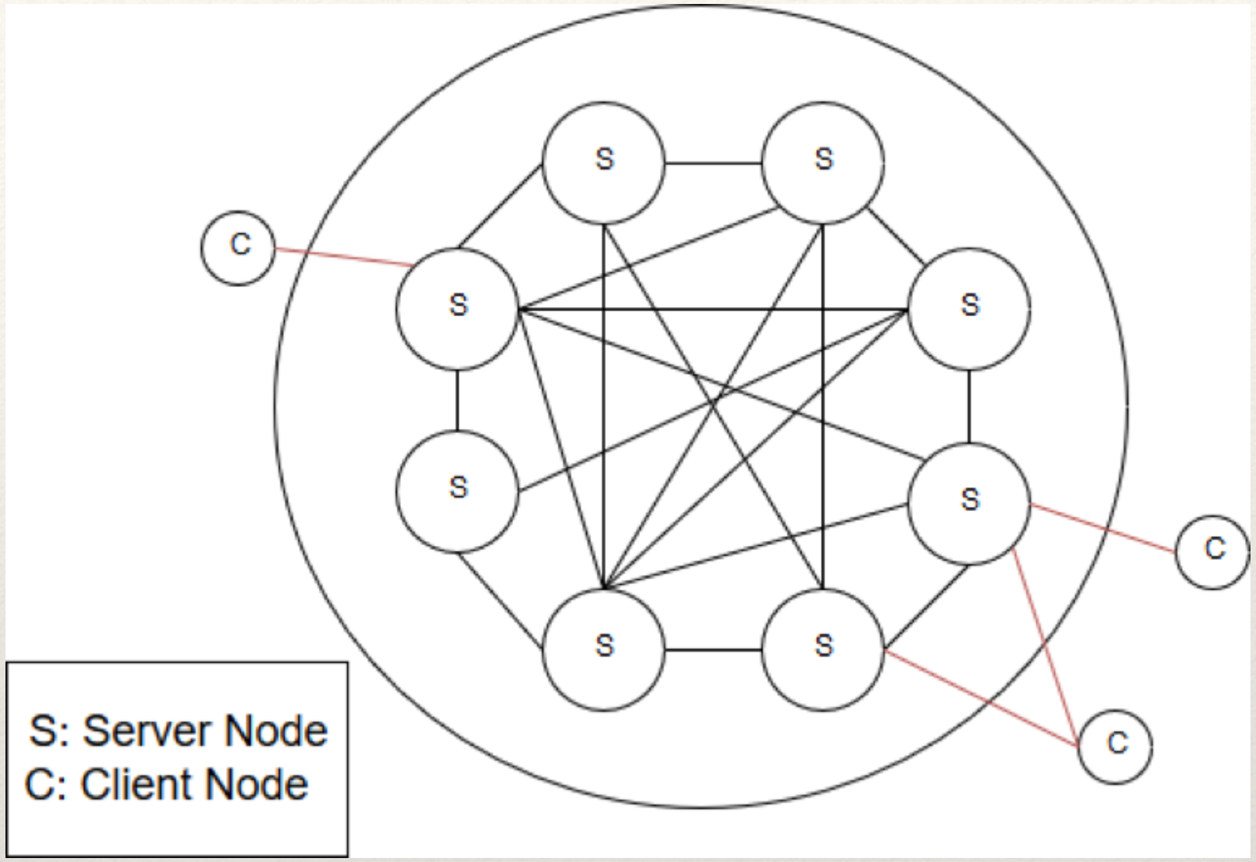
*Joint work (in progress) with Man Ho Au and Paulo Verissimo, 2018.

UNIVERSITÉ DU LUXEMBOURG

Challenge 4. Network analysis

Network attacks:

- Eclipse attack
- BGP Hijacking attack
- …



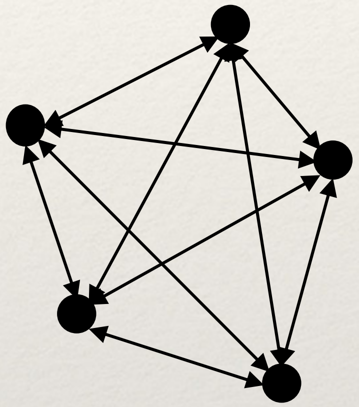
*Joint work (in progress) with Tong Cao, Jérémie Decouchant, Xiapu Luo, and Paulo Verissimo, 2018.

Challenge 5. Formal verification

Eventual consistency has been mechanically proved using simplified assumptions

Quiescent State

No Malicious Nodes



Clique Topology

Pîrlea, G. and Sergey, I. Mechanising blockchain consensus (CPP 2018).

Challenge 5. Formal verification

Challenge:

How to formally verify blockchain consensus with a realistic model and refined properties?
(Chain Quality, T-Consistency, malicious nodes, …)

*Joint work (in progress) with Cristian Mirto, Vincent Rahli, and Paulo Verissimo, 2018.

Thank you!

SNT
securityandtrust.lu
CRITIX

Jiangshan Yu

jiangshan.yu@uni.lu
www.jiangshanyu.com

CRITIX @SnT, *Critical and Extreme Security and Dependability*

We're hiring bright post-docs and research associates
willing to address these challenges!

UNIVERSITÉ DU LUXEMBOURG