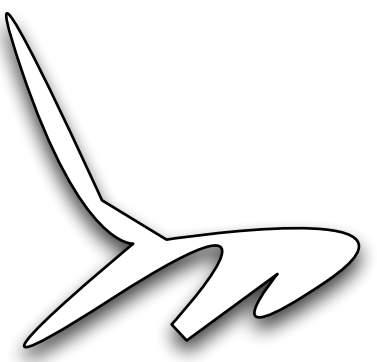
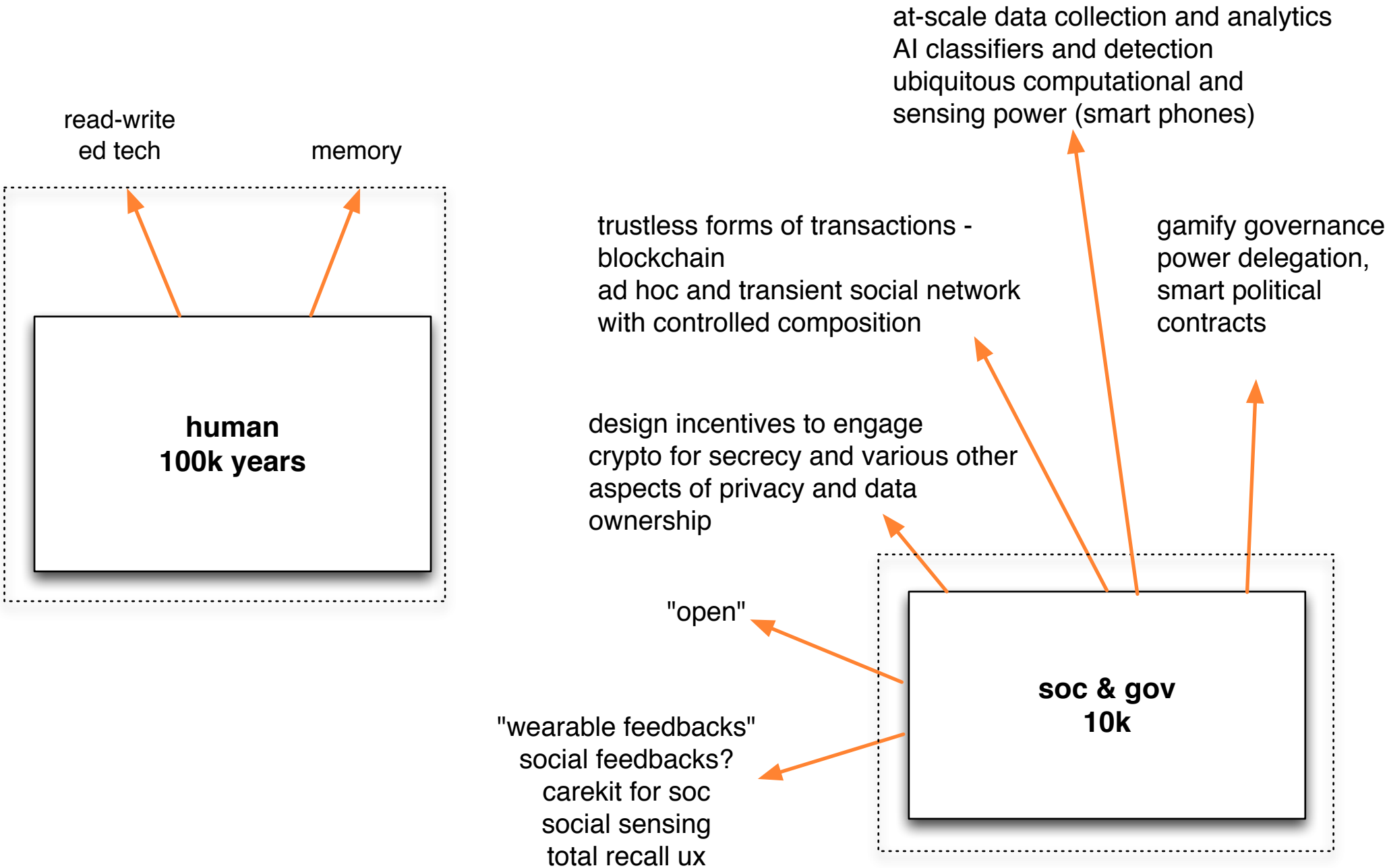
new social forms?

leverage for big questions




read-write
ed tech
memory
human
100k years
at-scale data collection and analytics
AI classifiers and detection
ubiquitous computational and
sensing power (smart phones)
trustless forms of transactions -
blockchain
ad hoc and transient social network
with controlled composition
gamify governance
power delegation,
smart political
contracts
design incentives to engage
crypto for secrecy and various other
aspects of privacy and data
ownership
"open"
"wearable feedbacks"
social feedbacks?
carekit for soc
social sensing
total recall ux
soc & gov
10k

The world **has become a lab** in a way it was not when Charles Fourier or Lenin proposed to engineer new social forms.

We can now study the "**quantified us**" not just the quantified self.

Let's see what we can engineer in terms of new governance with modern technological weapons

aware. I think mankind is more than waist-deep in daily routine. Countless inherited acts, accumulated pell-mell and repeated time after time to this very day, become habits that help us live, imprison us, and make decisions for us throughout our lives. These acts are incentives, pulsions, patterns, ways of acting and reacting that sometimes—more frequently than we might suspect—go back to the beginnings of mankind's history. Ancient, yet still alive, this multicenturied past flows into the present like the Amazon River pouring into the Atlantic Ocean the vast flood of its cloudy waters.

Braudel 1978

Government is a machine to integrate the social, emotional, and cognitive attributes of the group into a coherent, consensual, and prosperous whole - it is an ecosystem only partly of our own deliberate making.

Governance has to accomodate **psy**-**soc**-**cog** determinants that are somewhat immutable (think evolutionary psychology, eg the most frequent objection to communism being -it is nice, but it is not man) to the combinatorics of the possible (as sampled for instance by other living forms from beehives to complex bacterial biofilms).

(claim 1) Old forms of government

"immobilisme politique" - no substantial decision is taken

"etouffement bureaucratique" - dynamics of EU admin development

"opacite politique" constraints and architectural choices are opaque to the citizens, e.g. worn and wrong image of the redistribution model in France

"desengagement politique" participative gov is limited and stumbling on "click-time" problems - competing with neural marketing for cognitive wattage

"deep regulatory capture", eg the ongoing VW emissions defeat and car industry lobbying

"national borders" become inefficient anchors of national interest with other communities

(claim 2) New technologies are expanding on the possible, new schemes of governance are conceivable

new forms of: power delegation, citizen engagement, political contractuality, incentives.

at-scale data collection and analytics
powerful AI classifiers and detection
"open"
ubiquitous computational and sensing power (smart phones),
trustless forms of transactions - blockchain
creation of ad hoc and transient social network with controlled composition,
new methodologies for the design of incentives to engage in collectives,
cryptographic methods to handle secrecy and various other aspects of privacy and data ownership

education tech
game-derived techniques to cope with global problems (enhance/modify the individual - the boundary is unclear)
virtual worlds as labs for new forms of **emo**-**cog** and collective processes with different emergent governance models.

goals (see UN's subgoal SDG17)

examine and confront the said (gov-expansive) new techs
foster their recombination
use them to design new political ecosystems, new forms of governance or collective integration (intelligence, decision, action, monitoring),
think ahead the new forms of data and regulatory capture that will stand in the way

To foster experimental initiatives, discuss deployment, discuss their ressourcing (economics of new gov). To foster in a parallel theoretical thread, the reconceptualisation of the psy-soc-cog landscaping/political engineering needed to accompany the experimental design of new gov forms.

FR-UK workshop

26/05

25-26/05 -or- 1-2/06

citizen engagement/participative processes

collective intelligence (and limits/Dunbar)

NESTA:
argumentation/voting systems - new forms of representation delegation/liquid democracy

citizen-centric services
transcending frontiers
voting with taxes

gov in 20 yrs

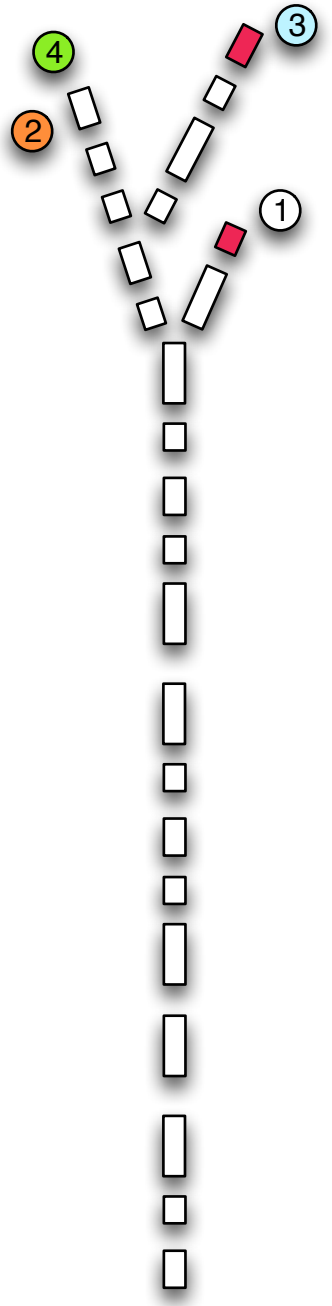
gamification of gov

reputation/mechanism design

transparency/trust/anonymity

stereotypes of politics - personalised political interaction

26/5 ecrire a étalab,



Blockchain

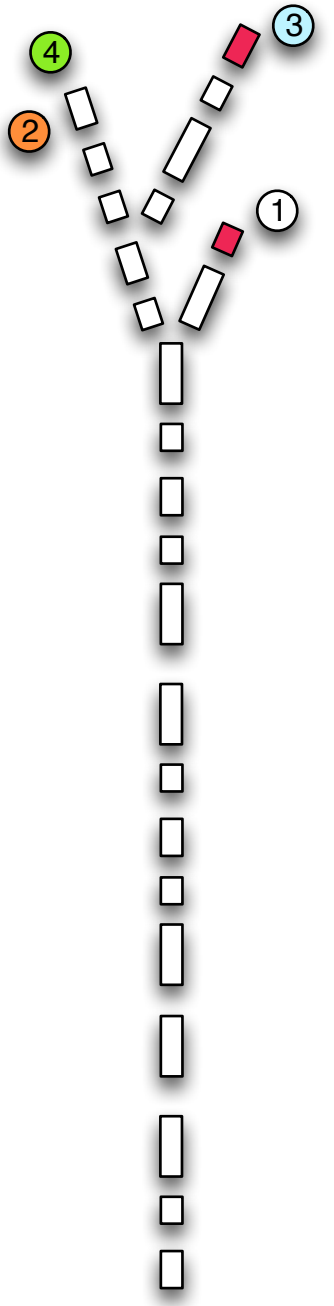
Vincent Danos

blockchain = consensus machine

maintain a distributed data-structure
with no central maintainer -

everyone can read
everyone can write
at any time

nodes do not know each other
everyone can join and quit



paradoxically - no intelligence more security

we take bitcoin - i.e. a crypto-currency as an example of a use of the blockchain algorithm data-structure = big collective bank account

but it is just an example

but it is a very good one:
- market cap USD 5B
- it is growing exponentially in some sense

- it is cognitively easy;
coherence is just no-double-spending

① how does it work (on paper)
what kind of security properties

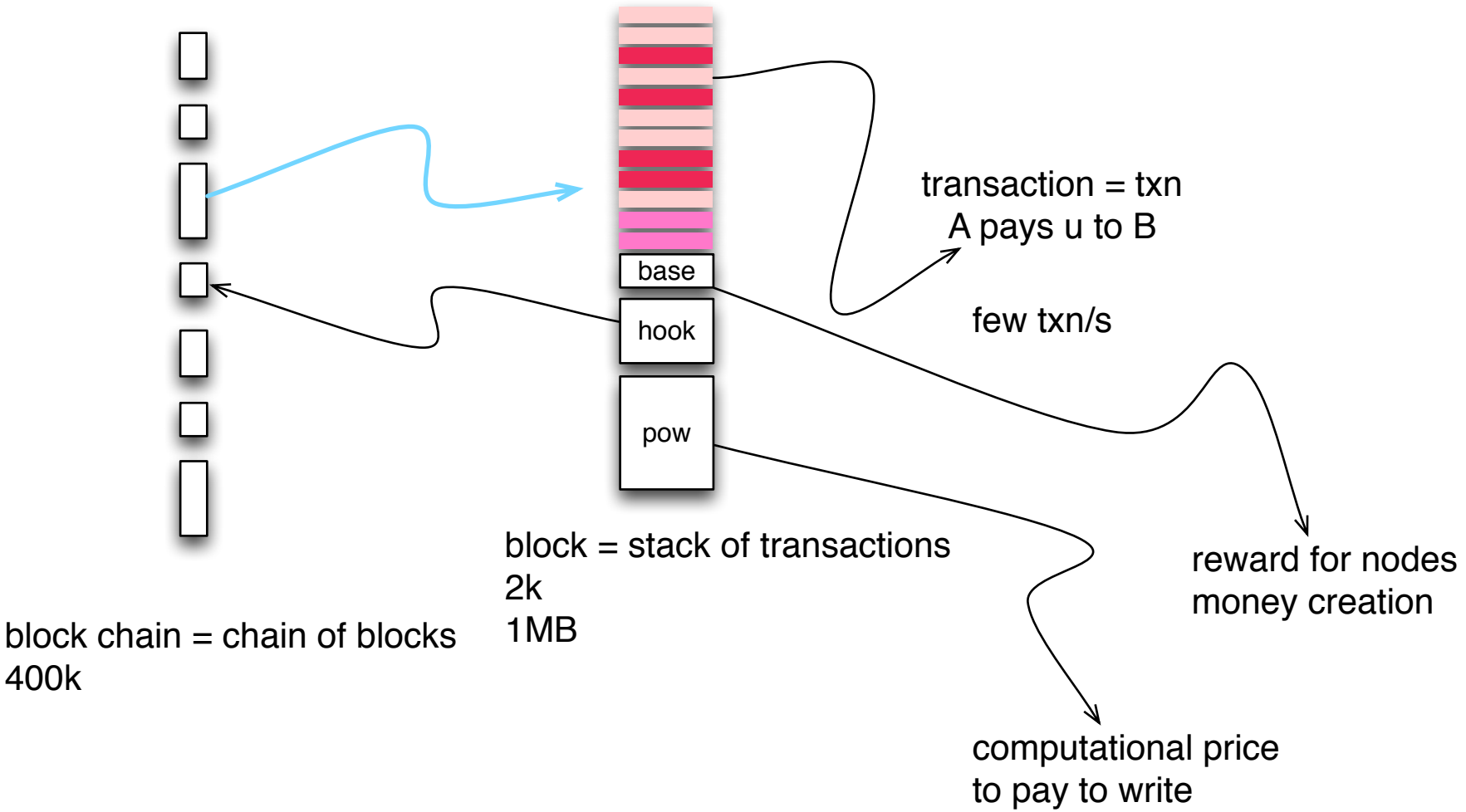
② how does it work in practice

③ why would nodes participate
economics of blockchain

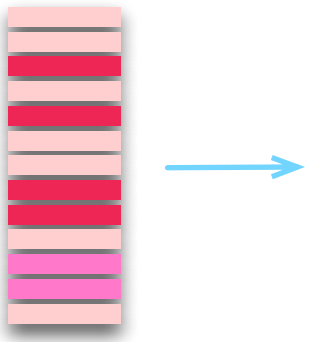
what comes next?

bitcoin's blockchain

maintain a distributed "accounting book" or ledger



blockhain local coherence



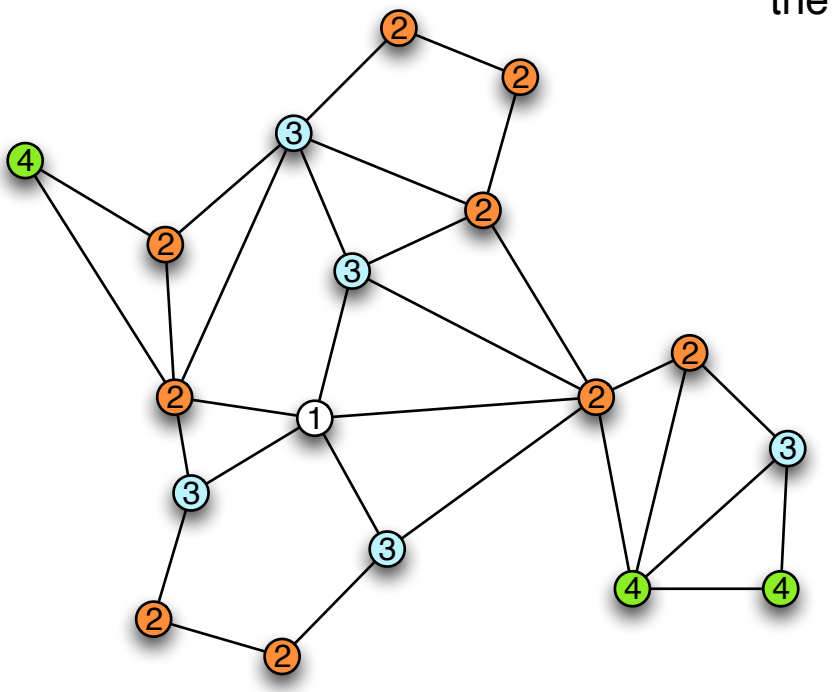
transaction = txn
A pays u to B

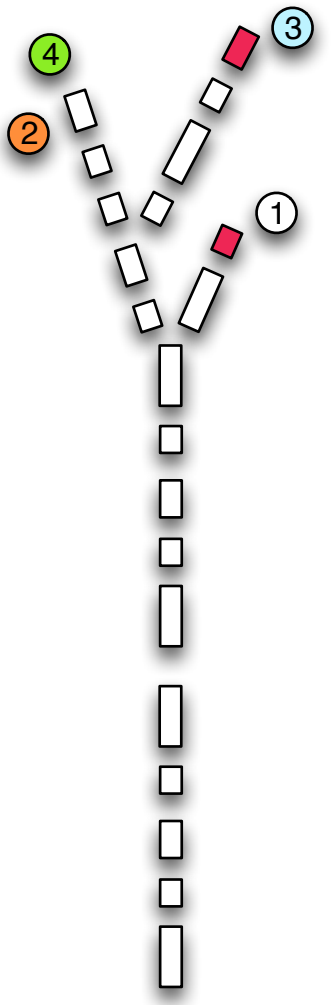
need to check authenticate (crypto signature)

need to check that the account A has ≥ u left

blockhain global coherence

global state of the system is a tree
the "head" is unstable





we cannot expect everyone
to have the same view of the world

nor can we expect everyone to play
according to the rules (open system)

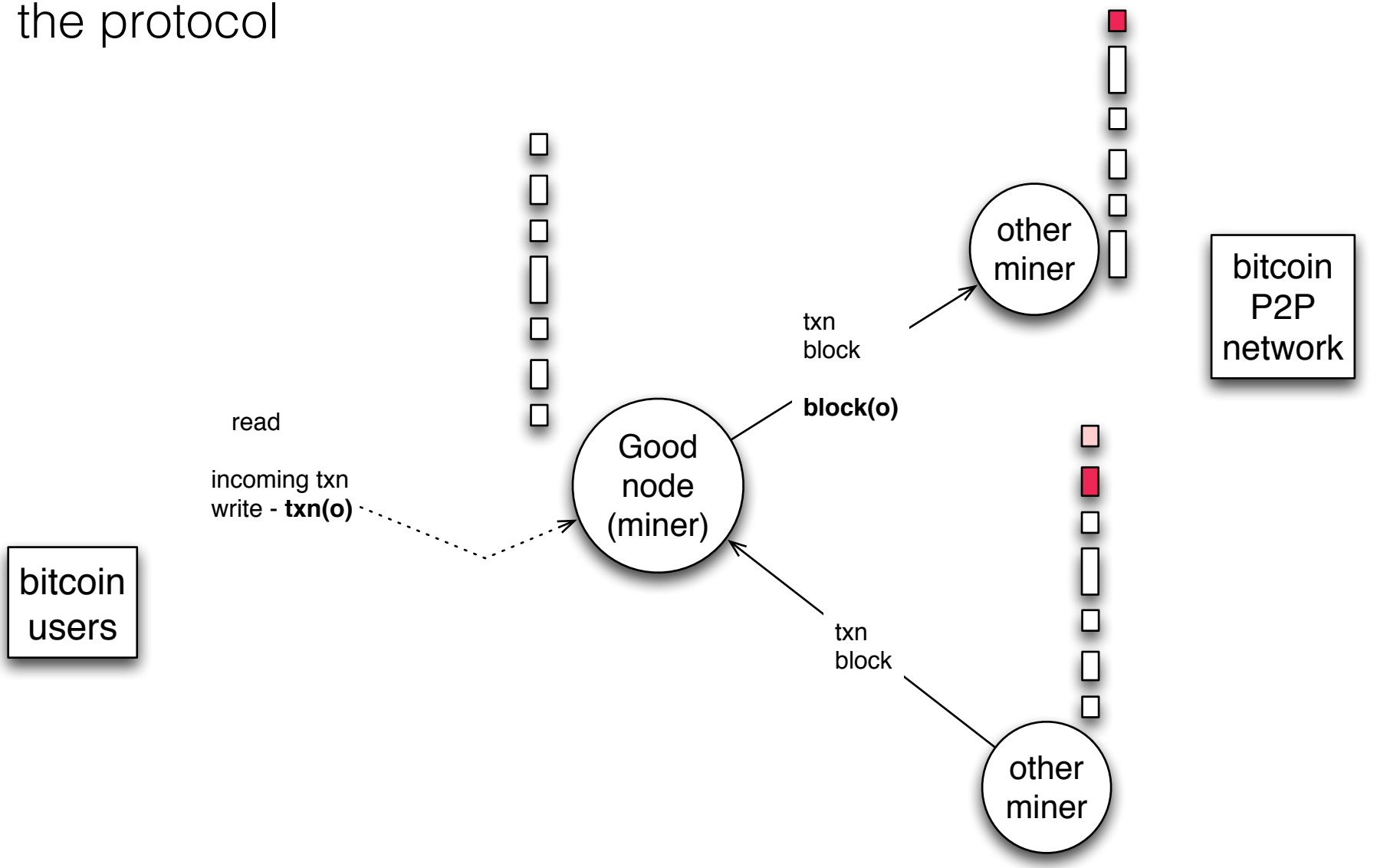
security properties

chain coherence - the probability of a fork at depth k is prop to 2^{-k}

chain quality - a lower bound on the number of blocks created by good guys on the chain (denial of service)

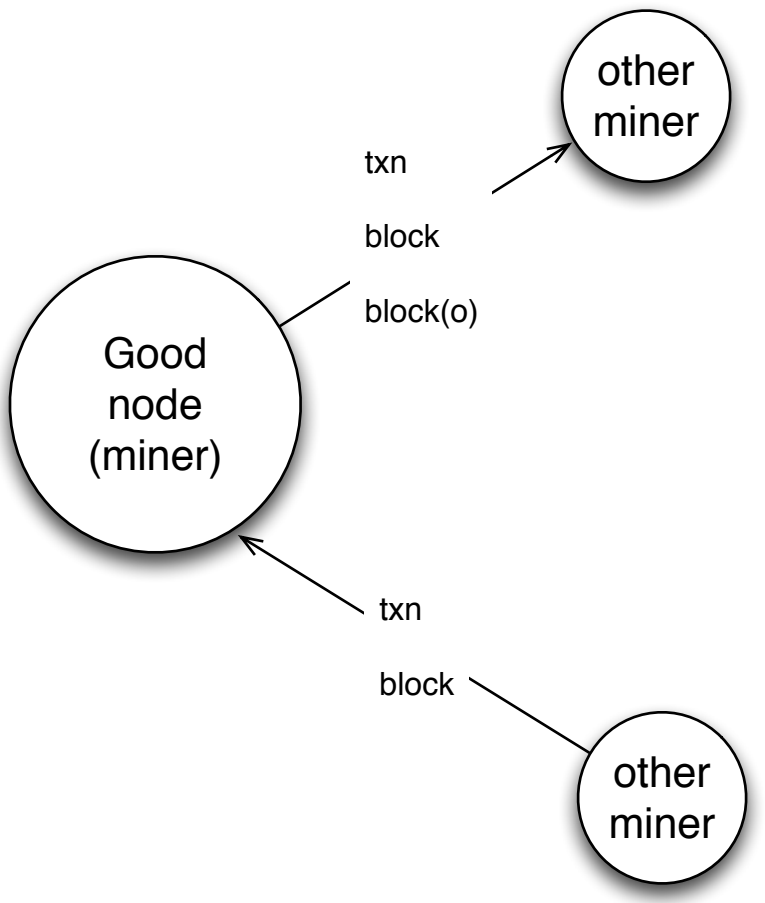
chain progress

the protocol



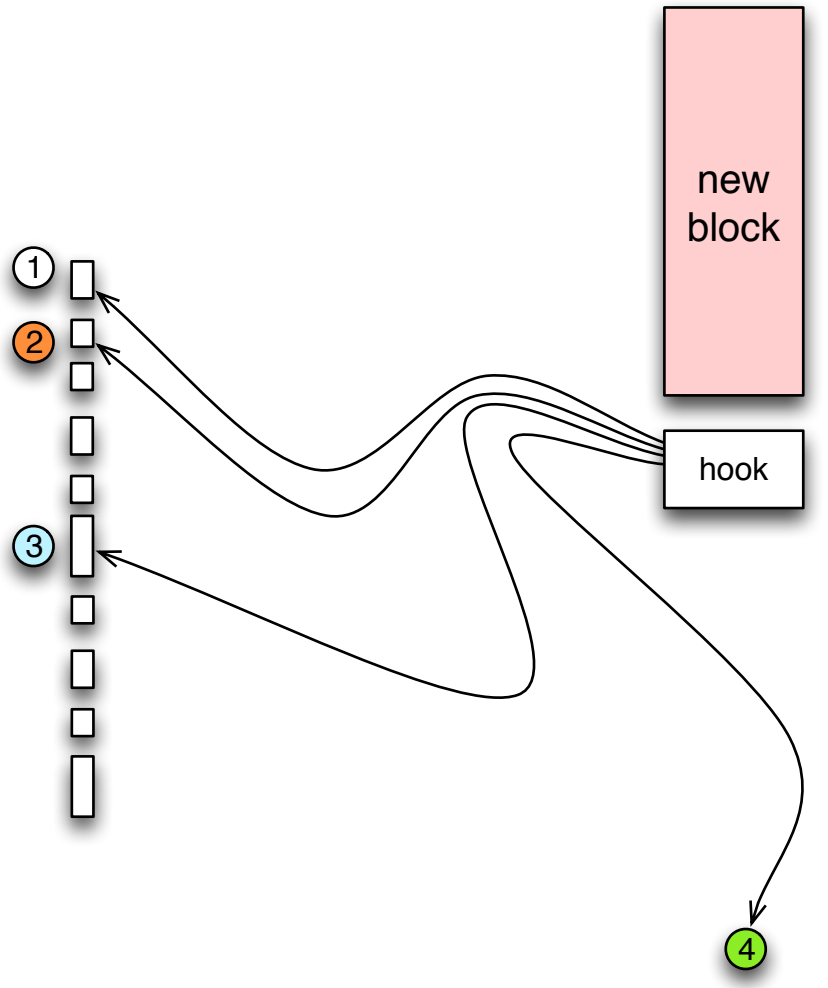
network-enforcement

only validated txn and blocks propagate



chain selection

what to do with a new block



security parameters

chain coherence, quality, progress

f = global block generation rate

T = characteristic time of propagation

fT = block generation per synchronisation round

a = good guys/bad guys ratio

for small fT and $a > 1 + x(fT)$
one has chain coherence

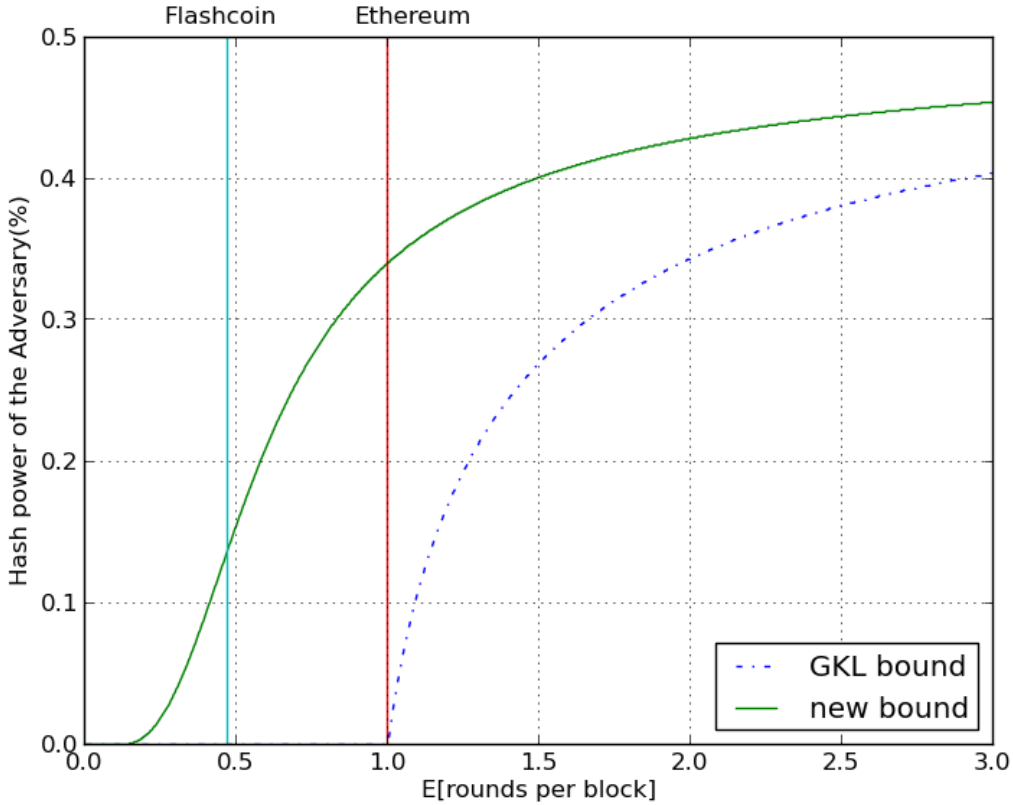
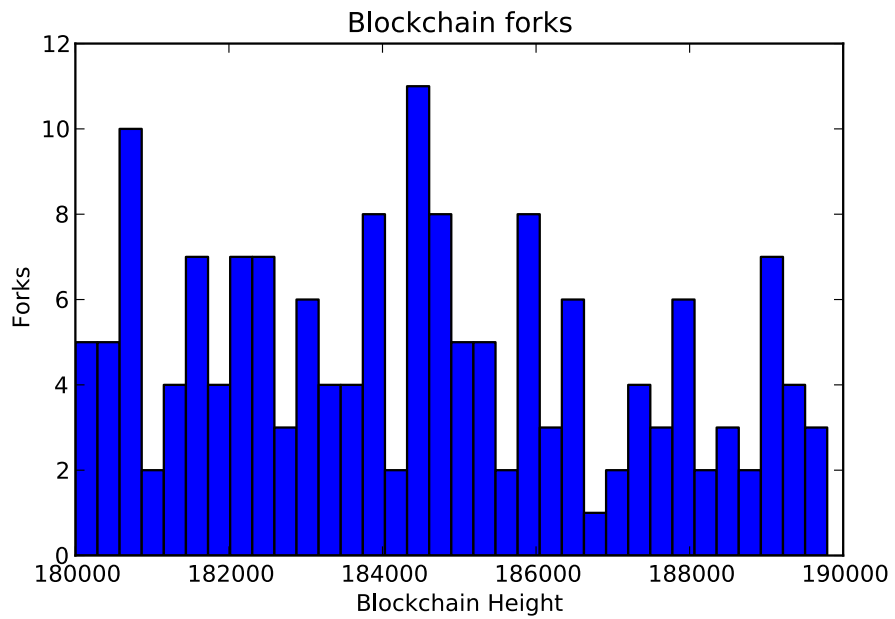


Fig. 3. The level of provable security comparing the results of [9] and our improved results for Bitcoin. Under the curves the common prefix property provably holds. The respective block-rate values chosen for two popular altcoins are depicted on the graph.

A. Kiayias et al, Nov 2015

with over 50% hash power,
adversary can rewrite the chain anywhere;

regrow the chain from depth before point of manipulation and when longer than current send top block around



Decker-Wattenhoffer, 2013

hence need to control fT

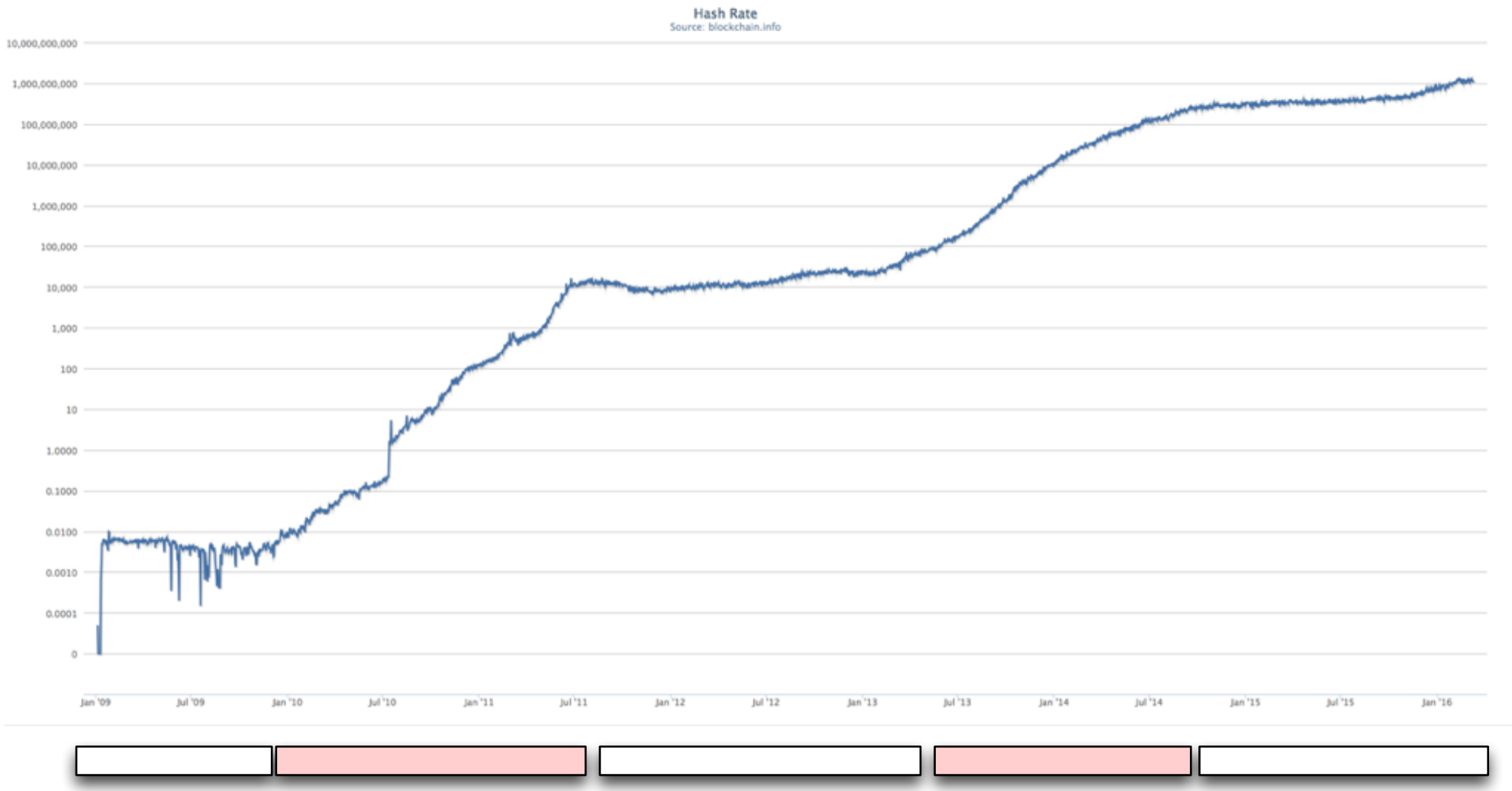
pow is a **thermostat** mechanism

pow = proof of work has a tuneable difficulty level

it is recomputed every 2 weeks (thermostat)
with target f = 10'
for a T = 10s

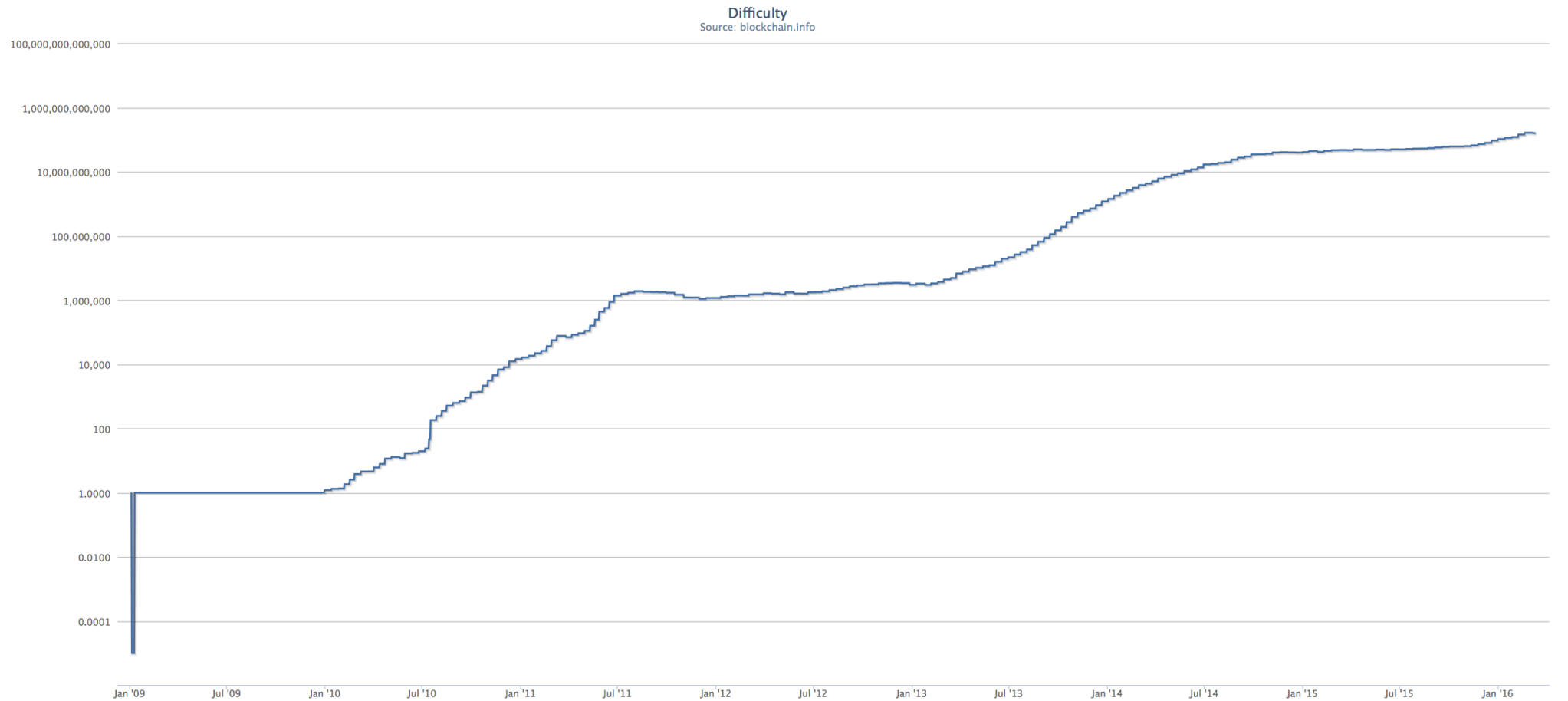
we are in the window where a ~ 1
= 50% attacker limit

bitcoin global hash power since Jan 09



https://blockchain.info/charts

thermostat at work



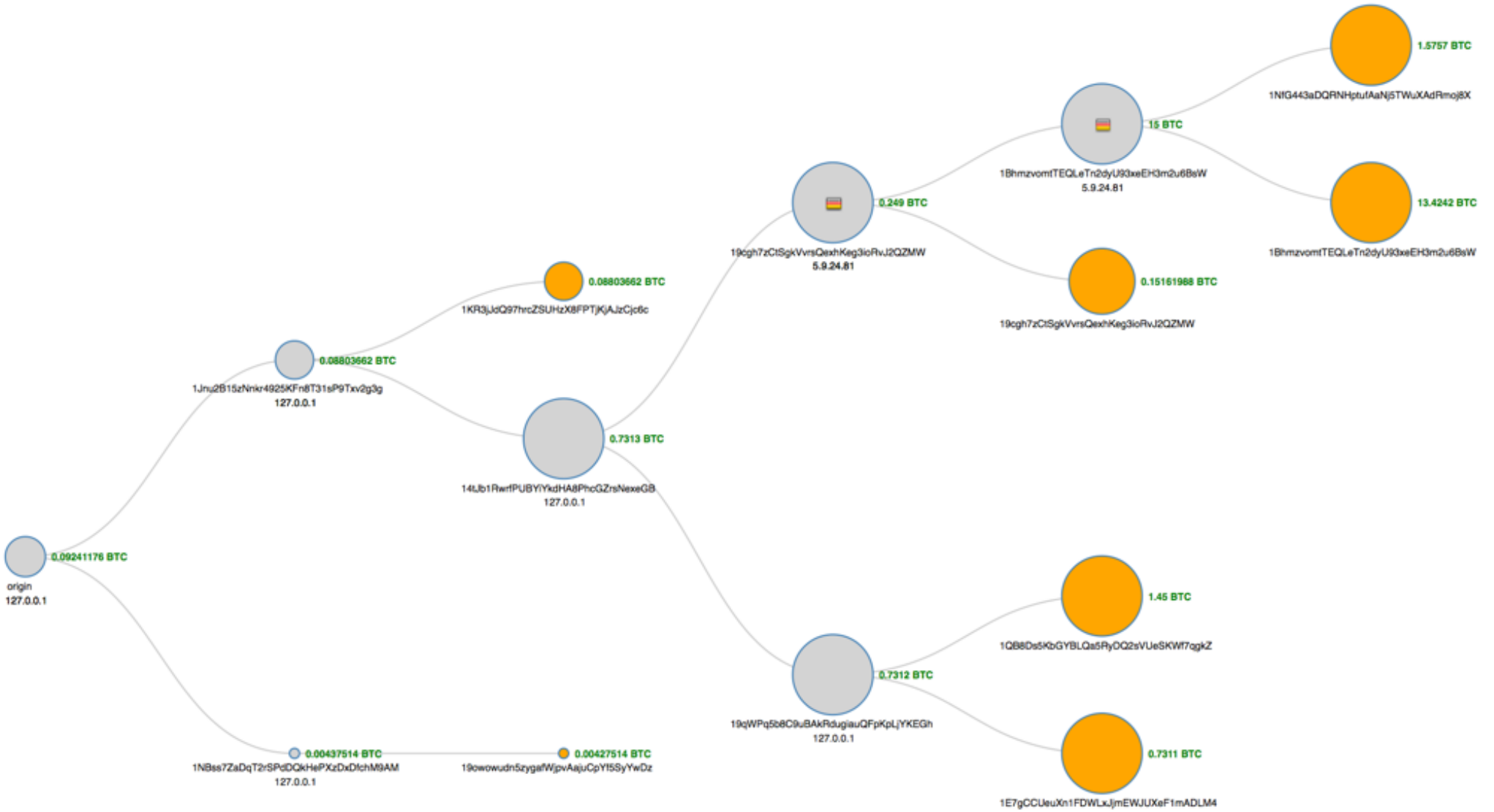
Transaction View information about a bitcoin transaction

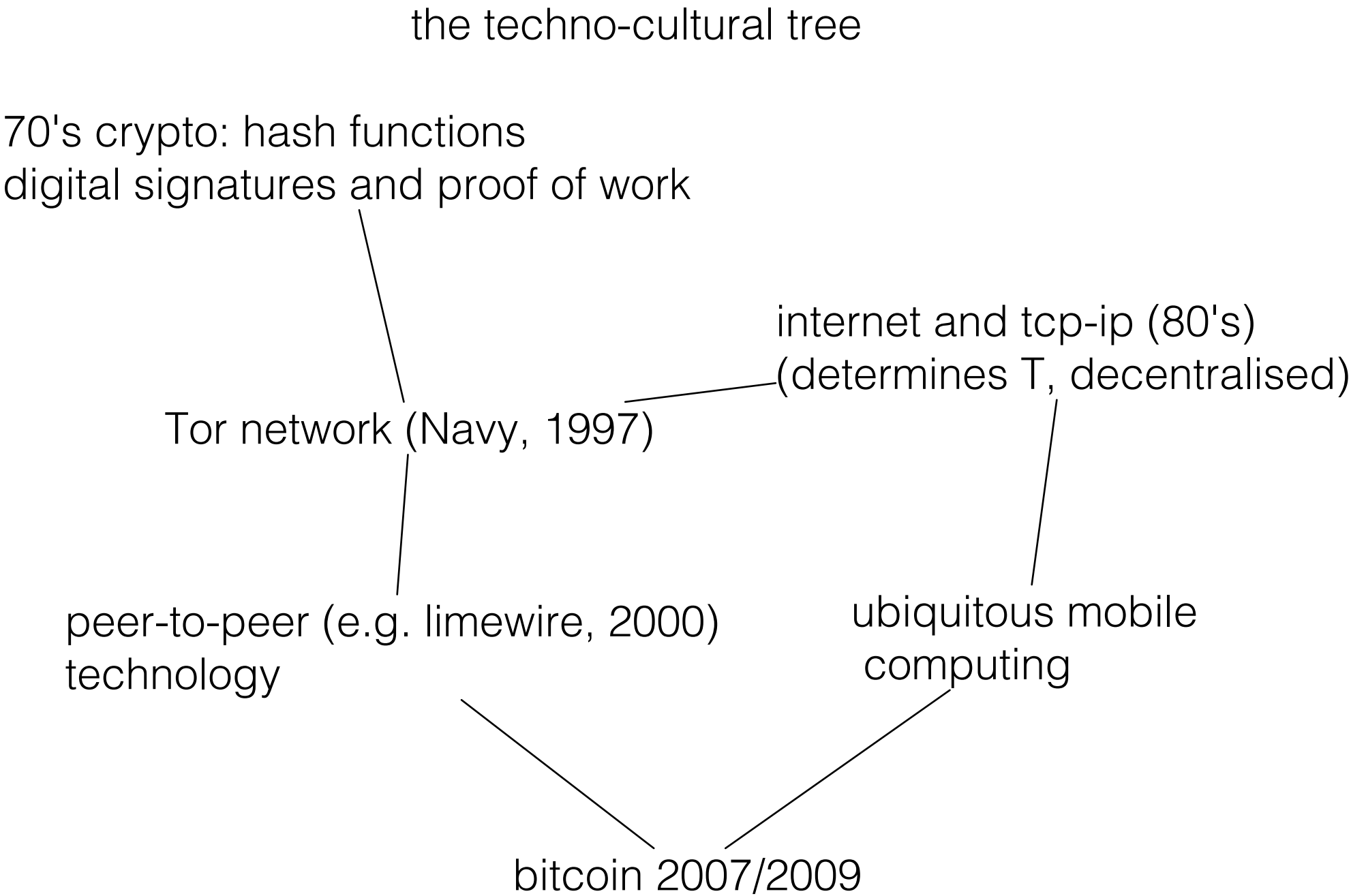
be34c3010b688a39183d9ec6b0da3fc8bbe62e5a136df9bfca4e695e0fa0a9f7

1NBss7ZaDqT2rSPdDQkHePXzDxDfchM9AM	1Jnu2B15zNnkr4925KFn8T31sP9Txv2g3g	0.08803662 BTC
	1NBss7ZaDqT2rSPdDQkHePXzDxDfchM9AM	0.00437514 BTC
		0.09241176 BTC

Summary	
Size	618 (bytes)
Received Time	2014-07-09 18:58:09
Included In Blocks	309976 (2014-07-09 19:05:01 + 7 minutes)
Confirmations	71870 Confirmations
Relayed by IP	Blockchain.info
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.09251176 BTC
Total Output	0.09241176 BTC
Fees	0.0001 BTC
Estimated BTC Transacted	0.08803662 BTC
Scripts	Show scripts & coinbase


origin
127.0.0.1
0.09241176 BTC
1Jnuj2B15zNnkr4925KFn8T31sP9Txv2g3g
127.0.0.1
0.08803662 BTC
1KR3jJdQ97hrcZSUHzX8FPTjKjAJzCjc6c
0.08803662 BTC
14tJb1RwrfPUBYiYkdHA8PhcGZrsNexeGB
127.0.0.1
0.7313 BTC
19cgh7zCtSgkVvrsQexhKeg3ioRvJ2QZMW
5.9.24.81
0.249 BTC
1BhmzvomfTEQLeTn2dyU93xeEH3m2u6BsW
5.9.24.81
15 BTC
1NfG443aDQRNHptufAaNj5TWuXAdRmoj8X
1.5757 BTC
1BhmzvomfTEQLeTn2dyU93xeEH3m2u6BsW
13.4242 BTC
19cgh7zCtSgkVvrsQexhKeg3ioRvJ2QZMW
0.15161988 BTC
19qWPq5b8C9uBAkRdugiauQFpKpLjYKEGh
127.0.0.1
0.7312 BTC
1QB8Ds5KbGYBLQa5RyOQ2sVUeSKWf7qgkZ
1.45 BTC
1E7gCCUeuXn1FDWLxJjmEWJUXeF1mADLM4
0.7311 BTC
1NBss7ZaDqT2rSPdDQkHePXzDxDfchM9AM
127.0.0.1
0.00437514 BTC
19owowudn5zygafWjpvAajuCpYf5SyYwDz
0.00427514 BTC


the techno-cultural tree
70's crypto: hash functions
digital signatures and proof of work
internet and tcp-ip (80's)
(determines T, decentralised)
Tor network (Navy, 1997)
peer-to-peer (e.g. limewire, 2000)
technology
ubiquitous mobile
computing
bitcoin 2007/2009

The anonymous Internet

Daily Tor users per 100,000 Internet users

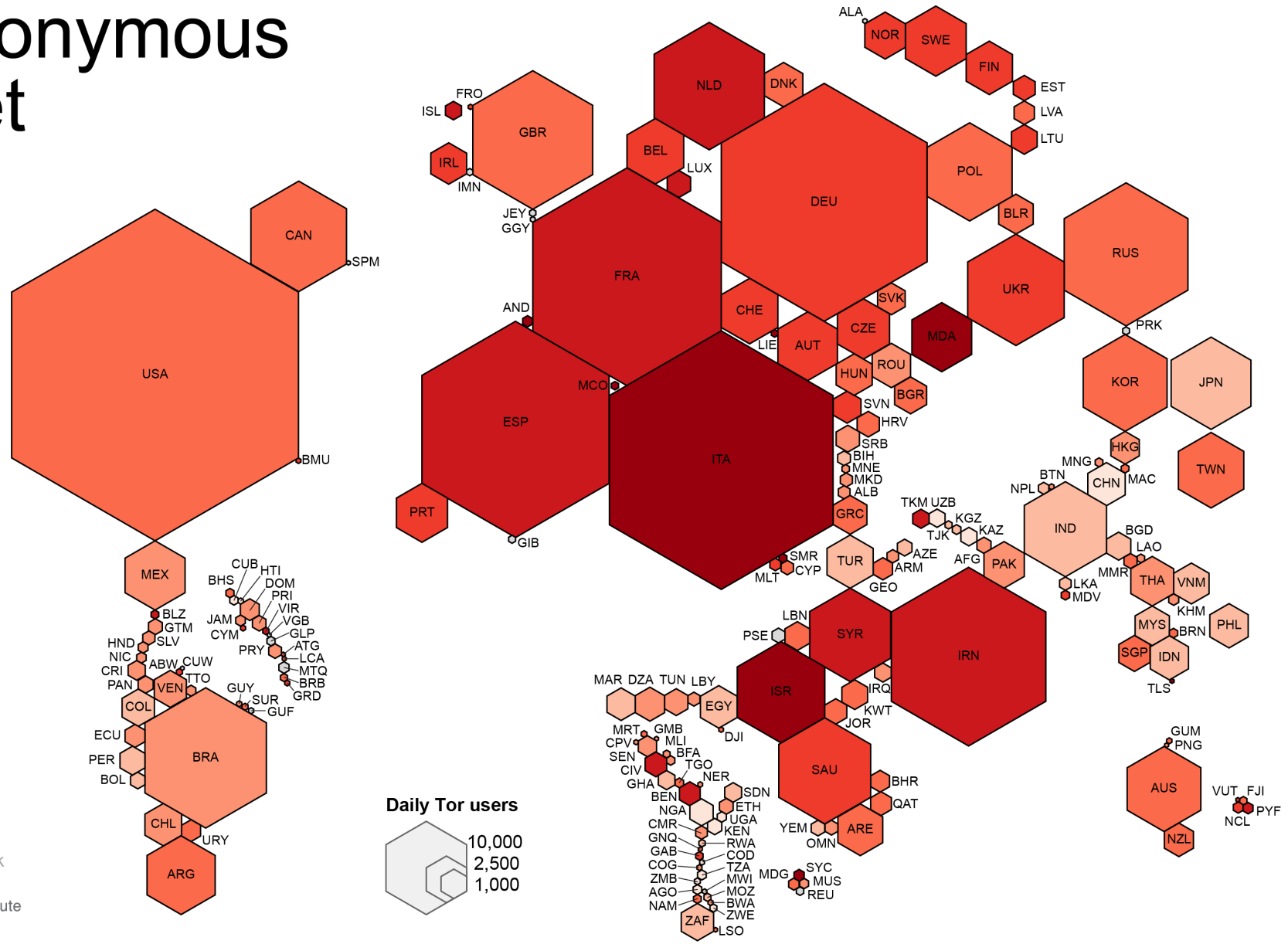
- > 200
- 100 - 200
- 50 - 100
- 25 - 50
- 10 - 25
- 5 - 10
- < 5
- no information

Average number of Tor users per day calculated between August 2012 and July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk

Oxford Internet Institute
University of Oxford



what comes next for BTC

security runs against speed

rates for btc processing 7/s (Paypal 115/s; Visa up to 50k/s)

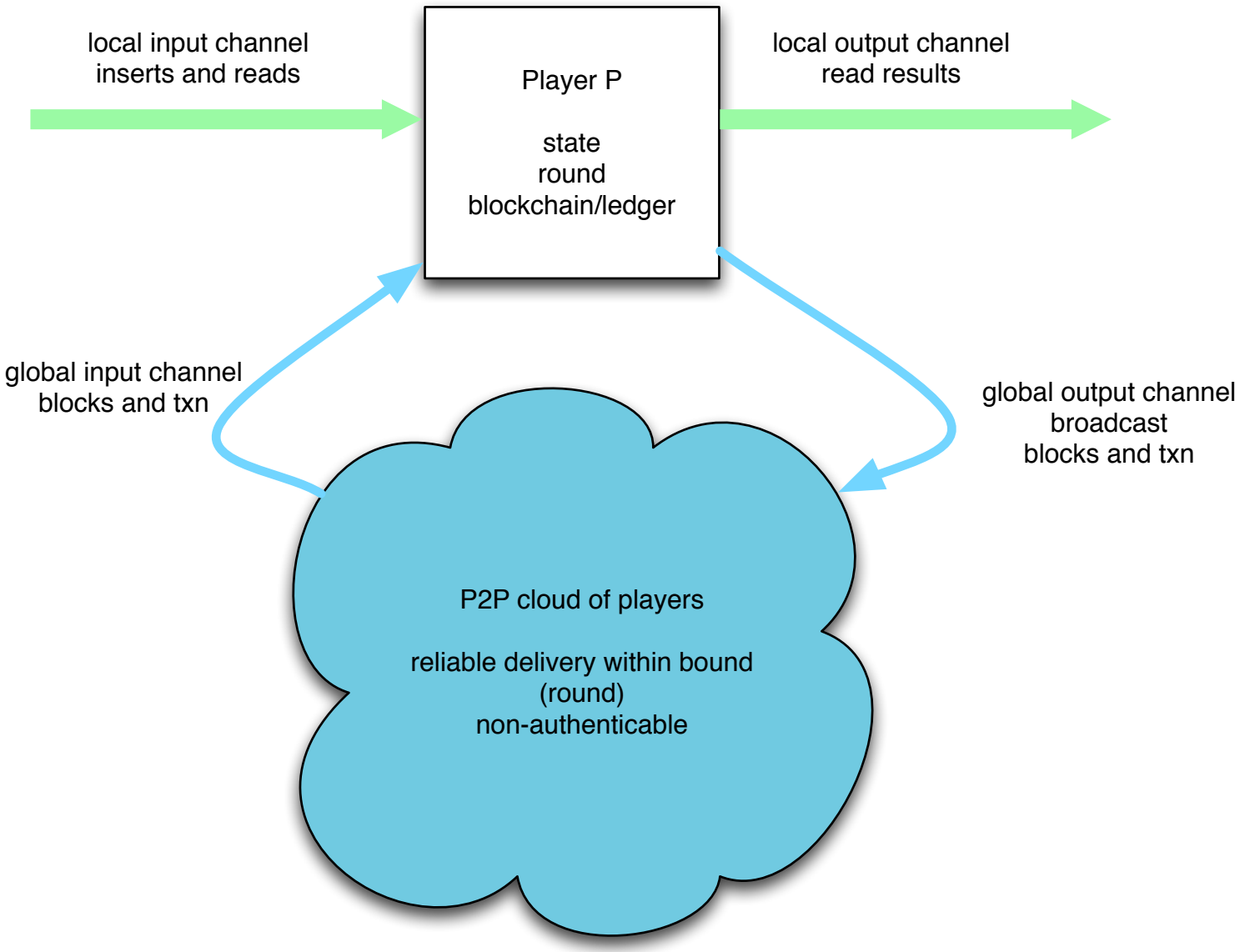
what comes next

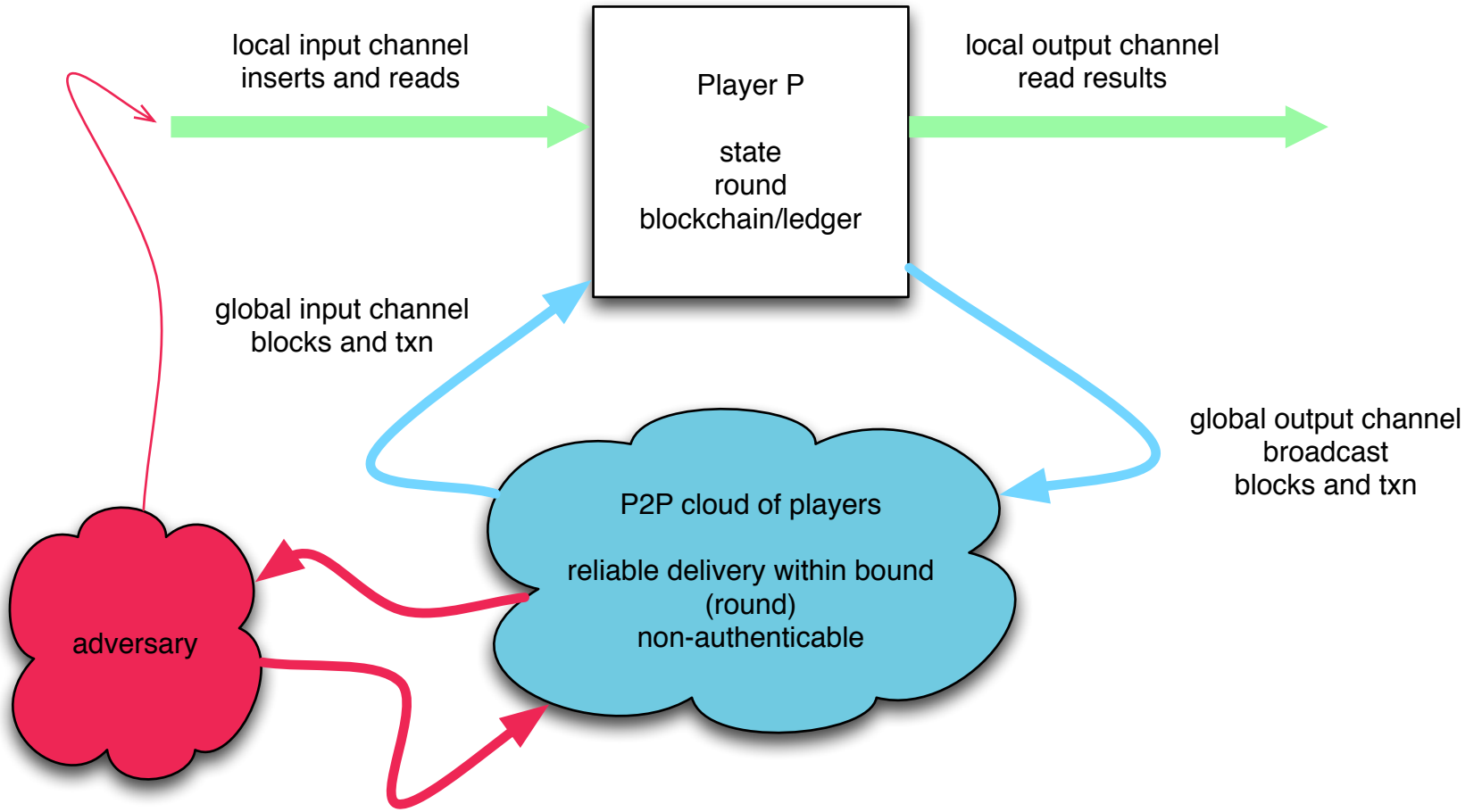
what do we want to write on a decentralised and **transparent** ledger?

what **incentives** do we give to nodes?

micro-payments?
supply chain?
facts?
deeds?
political contracts?

smart contracts


local input channel
inserts and reads
Player P
state
round
blockchain/ledger
local output channel
read results
global input channel
blocks and txn
global output channel
broadcast
blocks and txn
P2P cloud of players
reliable delivery within bound
(round)
non-authenticable


local input channel
inserts and reads
Player P
state
round
blockchain/ledger
local output channel
read results
global input channel
blocks and txn
global output channel
broadcast
blocks and txn
P2P cloud of players
reliable delivery within bound
(round)
non-authenticable
adversary