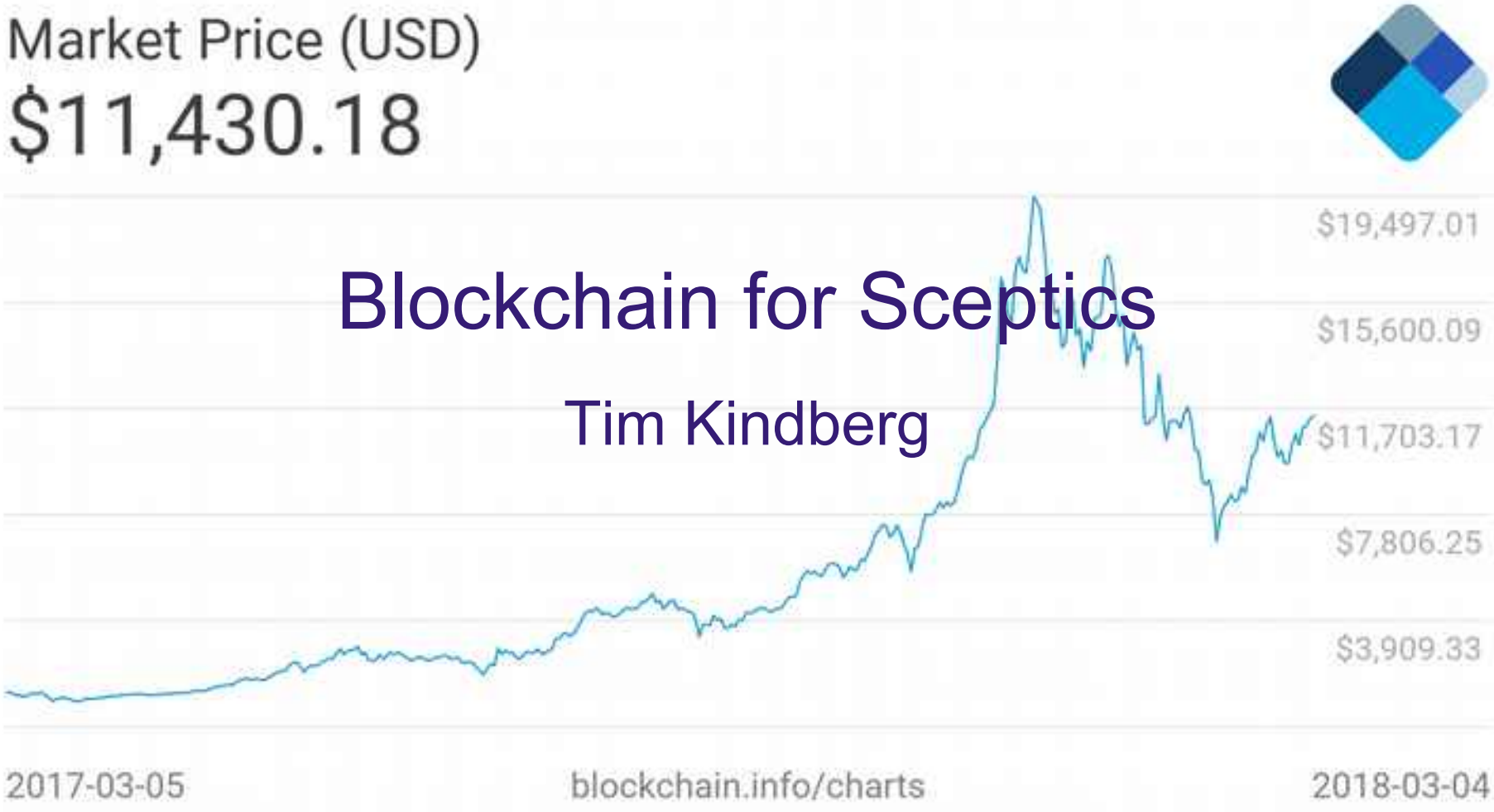
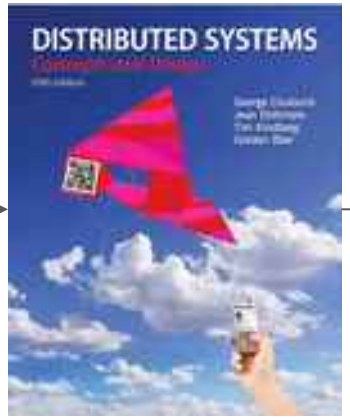


Blockchain for Sceptics

Tim Kindberg

about me



HEWLETT PACKARD

pervasive media studio

SCREEN

BBC

VORD

ORACLE

distributed / mobile / pervasive / urban computing

For Sceptics

Understanding and analysis of what is asserted to be true

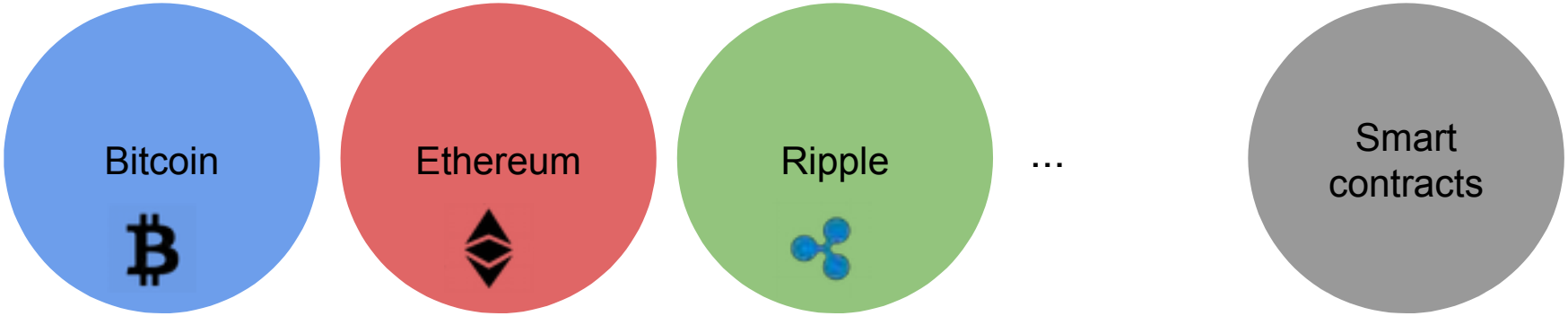
Questioning of agendas

Creative response

Scepticism (evidence) vs cynicism (outlook)

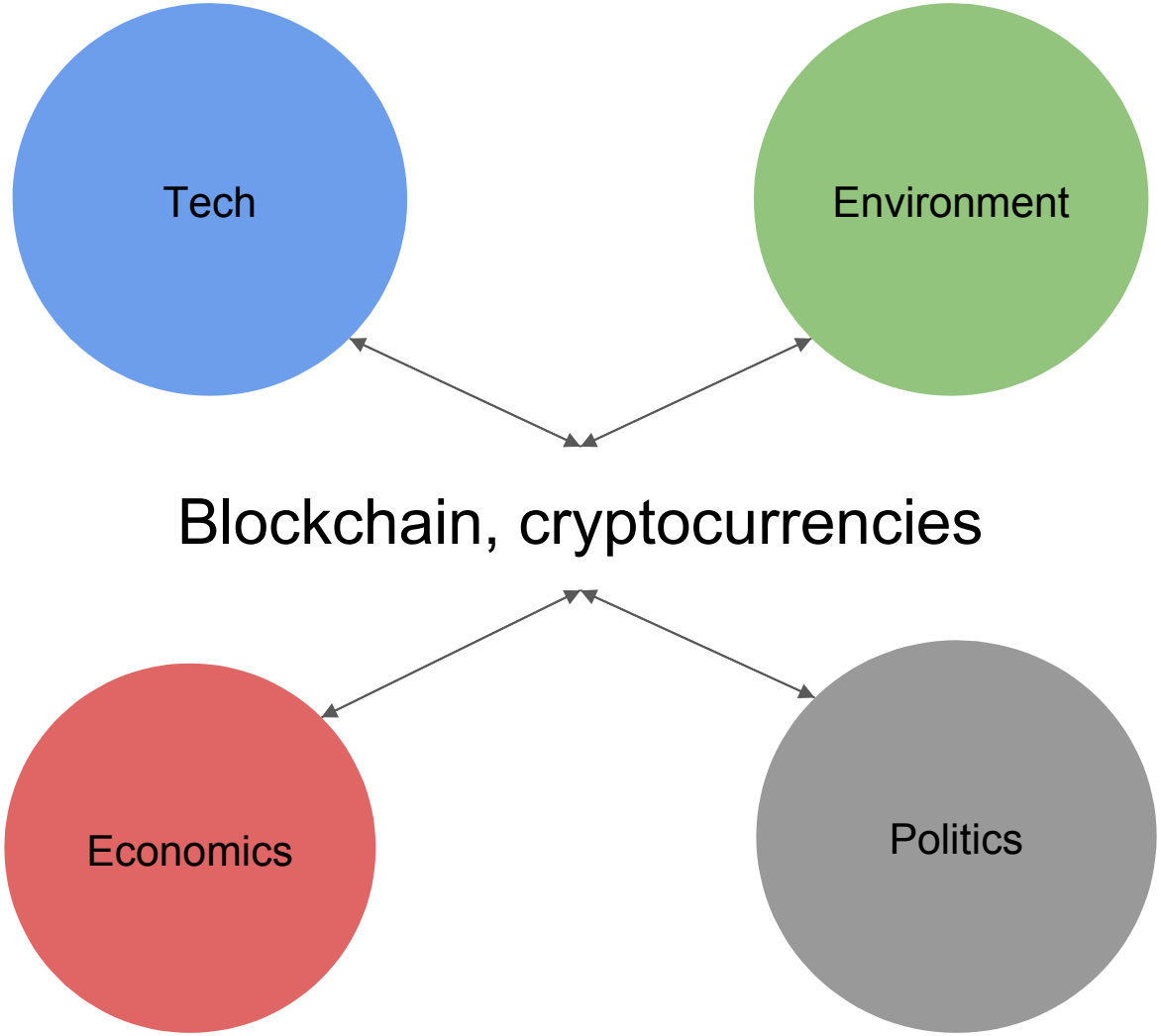
Tradition in science, philosophy

cryptocurrencies



Blockchain

Ledgers for transactions
Commerce, governance,... independent of institutions


Tech
Environment
Blockchain, cryptocurrencies
Economics
Politics

Bitcoin

Nakamoto, 2008

Goals for digital currency ("cryptocurrency")

Replace physical tokens (coins, notes, cards) with bits and software

Decentralise transactions - no trusted third parties (gov't, financial institutions)

Low transaction fees

Pseudonymity / anonymity


Bank of England
AK47 900731
Five Pounds
I have nothing to offer but blood, toil, tears and sweat
£5
AK47 900731

Digital currency, ledgers

'nocoin' = data e.g. [AK47900731, 5NOC]

Double-spending problem: *A* pays same *nocoin* to *B* and *C*

Prevent with a **Ledger**:

Append-only, immutable, public record of transactions

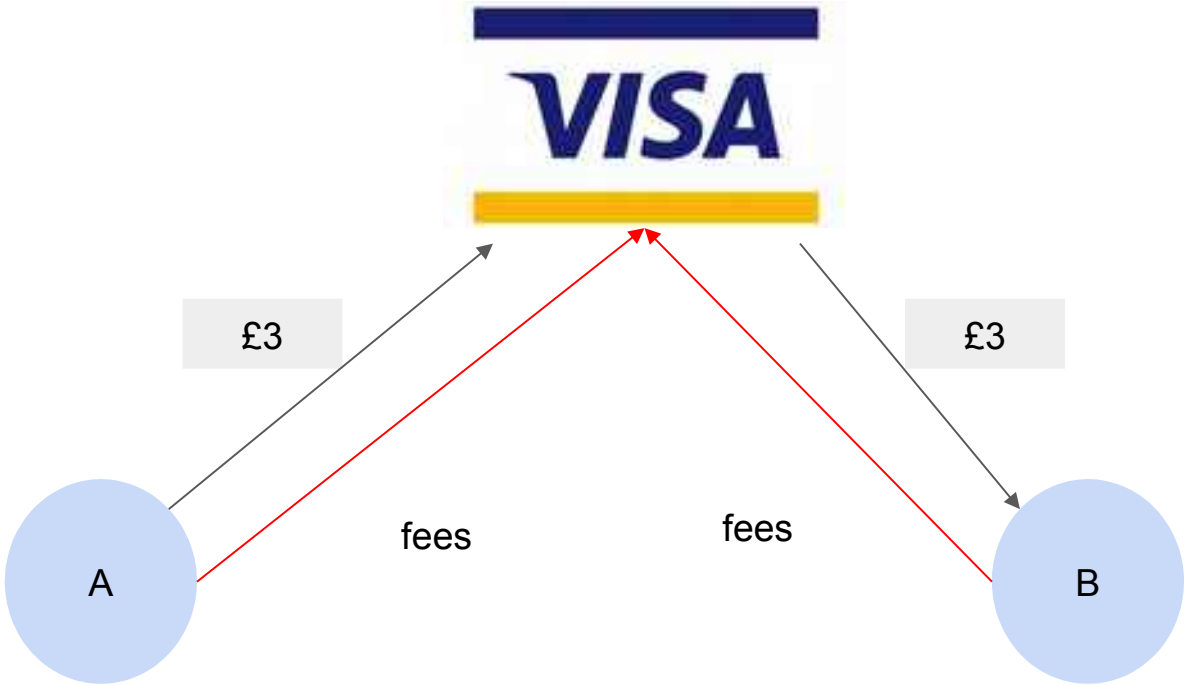
Whichever appears first for a given nocoin from A 'wins'

AL73077409, U→X
AK47900731, A→B
AK48300542, V→Z
….

Ledger

Visa Transaction

A pays B £3

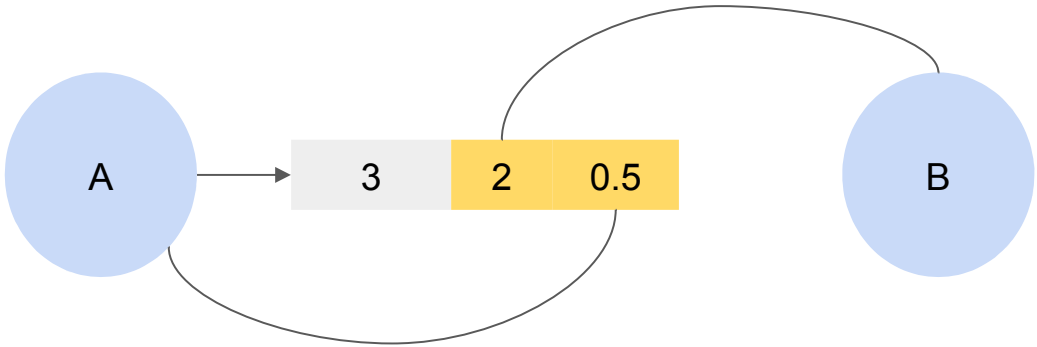


Bitcoin Transaction

inputs are previous transactions paying bitcoins to *A*

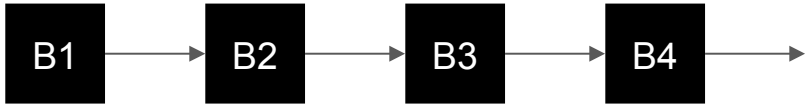
outputs pay bitcoins to others (possibly including *A*)

Difference is a transaction fee



Digital ledger

Ledger = **blockchain**



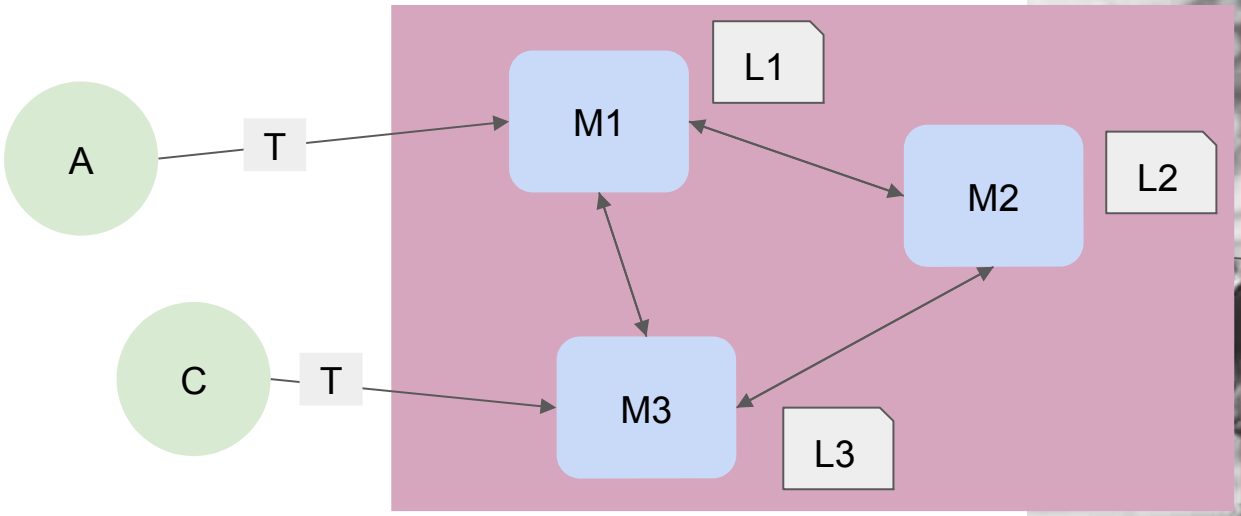
Digital equivalent of indestructible physical ledger written in permanent ink

Each block contains transactions in order, like a page in a real ledger

Can't change/delete/reorder blocks (they're cryptographically linked)

Anyone can read, but identifiers anonymised (Jo Smith → 341878234730)

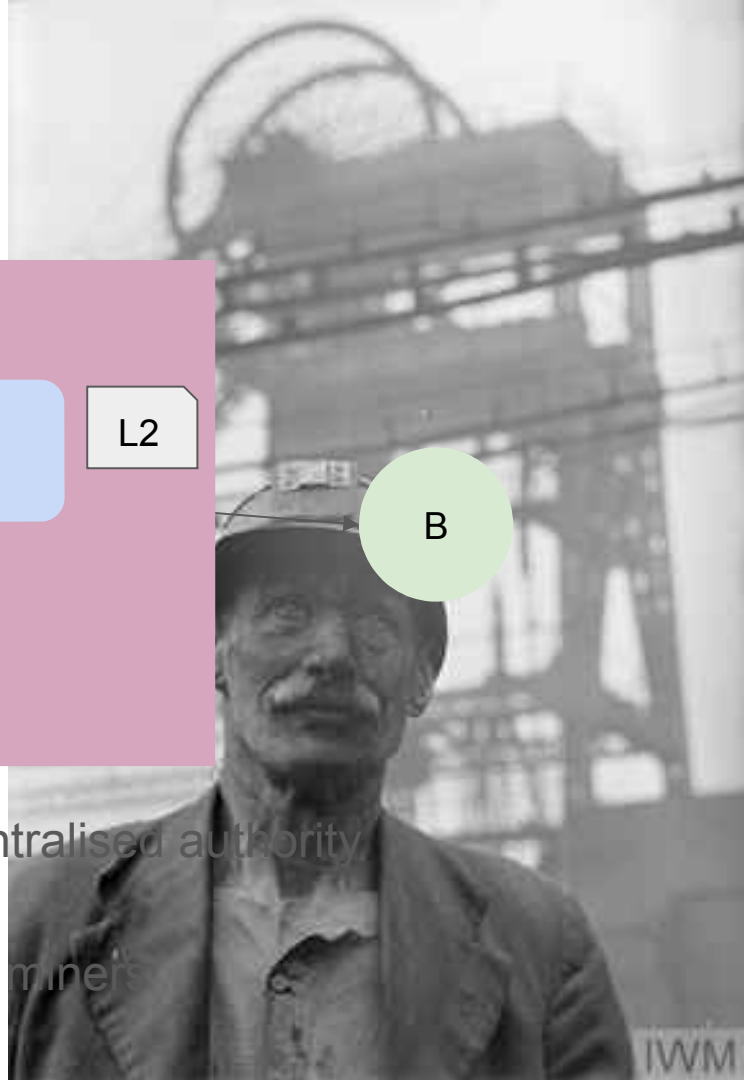
Decentralised ledger



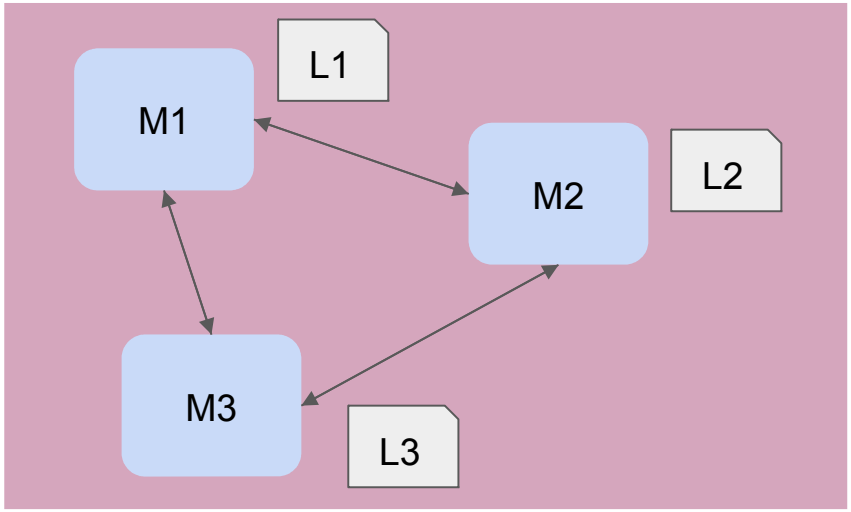
Collection of **miners** cooperate, instead of centralised authority

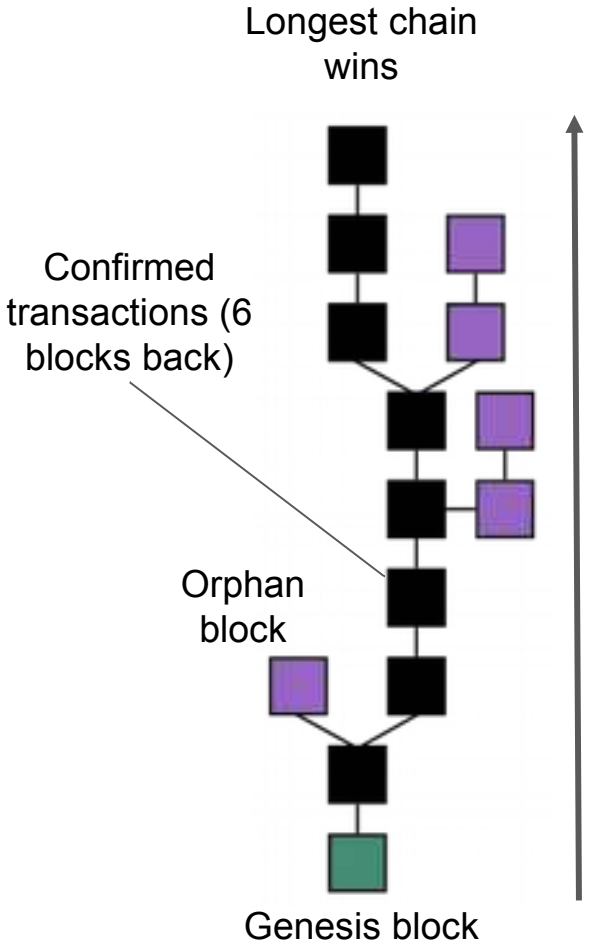
Add blocks of transactions to ledger

Forward transactions and new blocks to other miners



Distributed Consensus





Copies of the ledger are independently updated

But must agree eventually

Bad guys

Present different ledgers to *B* and *C* with transaction order reversed. *B* b[illegible]eves has *A*'s money, and so does *C*

Incentivise good behaviour: if *M* 'mines' a new block, rewa[illegible]n n[illegible] bitcoins - on top of transaction fees

Proof of work: significant computation to mine a block (

[illegible]*n* for[illegible]k *B* s[illegible]t h[illegible](*n* +[illegible]*d* (diffic[illegible]

[illegible]om[illegible]e p[illegible]er[illegible]goo[illegible] > [illegible]% o[illegible]ta[illegible]ad gu[illegible]

Numbers (Mar 2018) https://bitinfocharts.com/

Bitcoin blockchain size: c. 190GB

Block creation rate: 1 per 10 minutes (normative)

Mining difficulty adjusted every 2016 blocks

Price volatility 5-10 times higher than gold & major currencies

Active addresses/24hr: c. 700,000

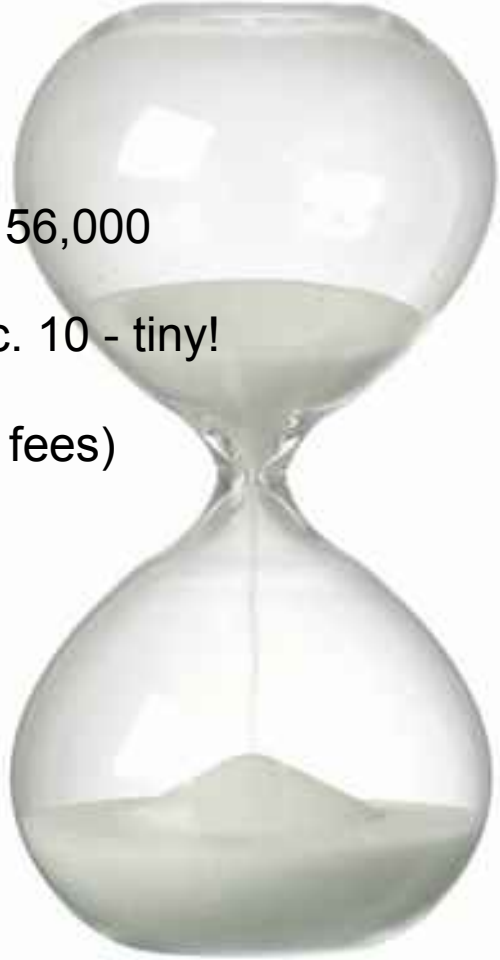
50% less mined BTC every 210,000 blocks (4 years) => cap of 21,000,000BTC

Numbers (Mar 2018)

Visa: average about 1,500 transactions per second, up to 56,000

Bitcoin: about 2 transactions per second worldwide, max c. 10 - tiny!

Long and unpredictable transaction delays (depending on fees)



Reflections

Questions

Does Blockchain scale? (No)

Are Blockchain transaction costs low - cup of coffee? (No - see above)

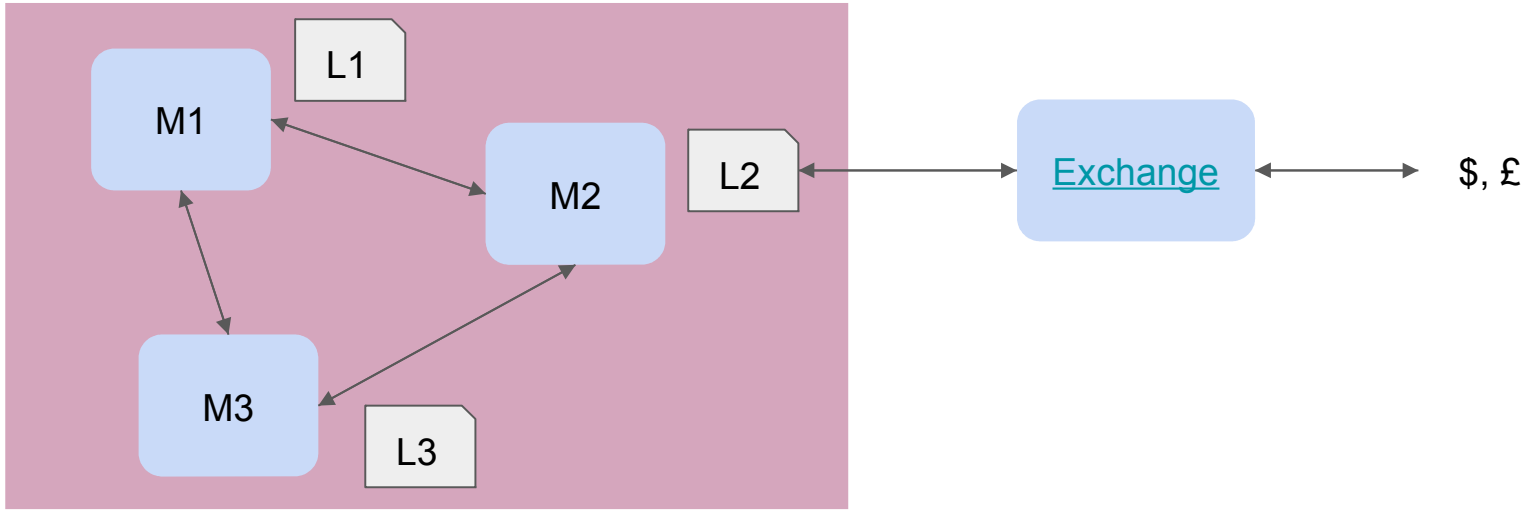
Preserves anonymity? (Don't count on it)

Is Blockchain provably correct? (Maybe) Secure? (No - exchanges hacked)

Does Blockchain eliminate trusted third parties? (No)

Is Blockchain fit for an era of global warming? (No)

Third parties: exchanges and miners



Miners: wealthy, pseudonymous, few and motivated to game the system

Trust? Game theory and cryptoanalysis as opposed to reputation

Global warming

Mining (proof of work) burns a lot of electricity (debate)

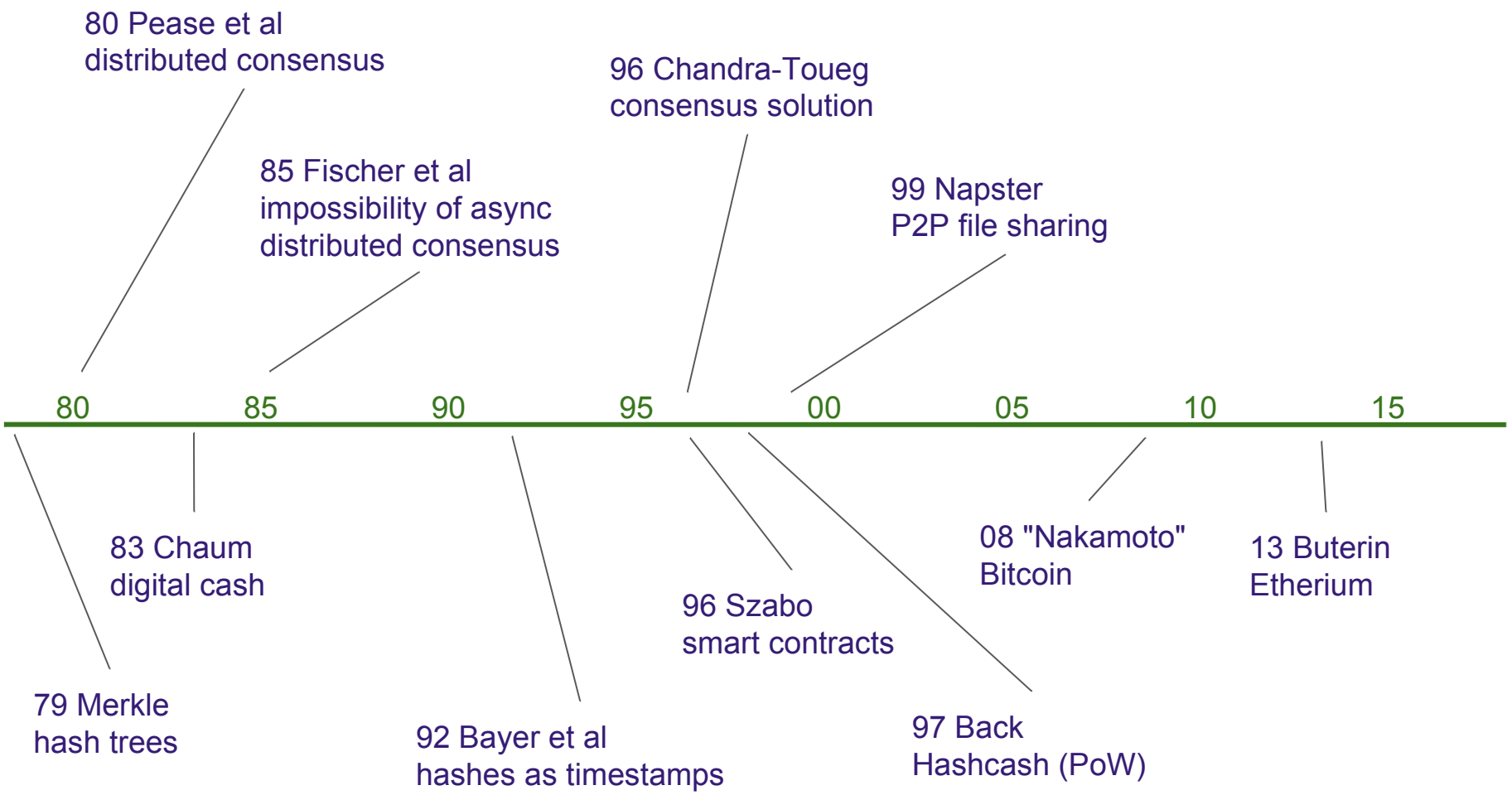
Estimates 0.1 - 3.4GW, or 0.9 - 30.1 TWh/year

The work performed is meaningless in itself

It's early days, right?

Nope, Distributed Consensus has been a topic of research since early 1980s

It's hard. And an economically embedded protocol is harder


80 Pease et al
distributed consensus
85 Fischer et al
impossibility of async
distributed consensus
96 Chandra-Toueg
consensus solution
99 Napster
P2P file sharing
80
85
90
95
00
05
10
15
79 Merkle
hash trees
83 Chaum
digital cash
92 Bayer et al
hashes as timestamps
96 Szabo
smart contracts
97 Back
Hashcash (PoW)
08 "Nakamoto"
Bitcoin
13 Buterin
Etherium

What's new about blockchain?

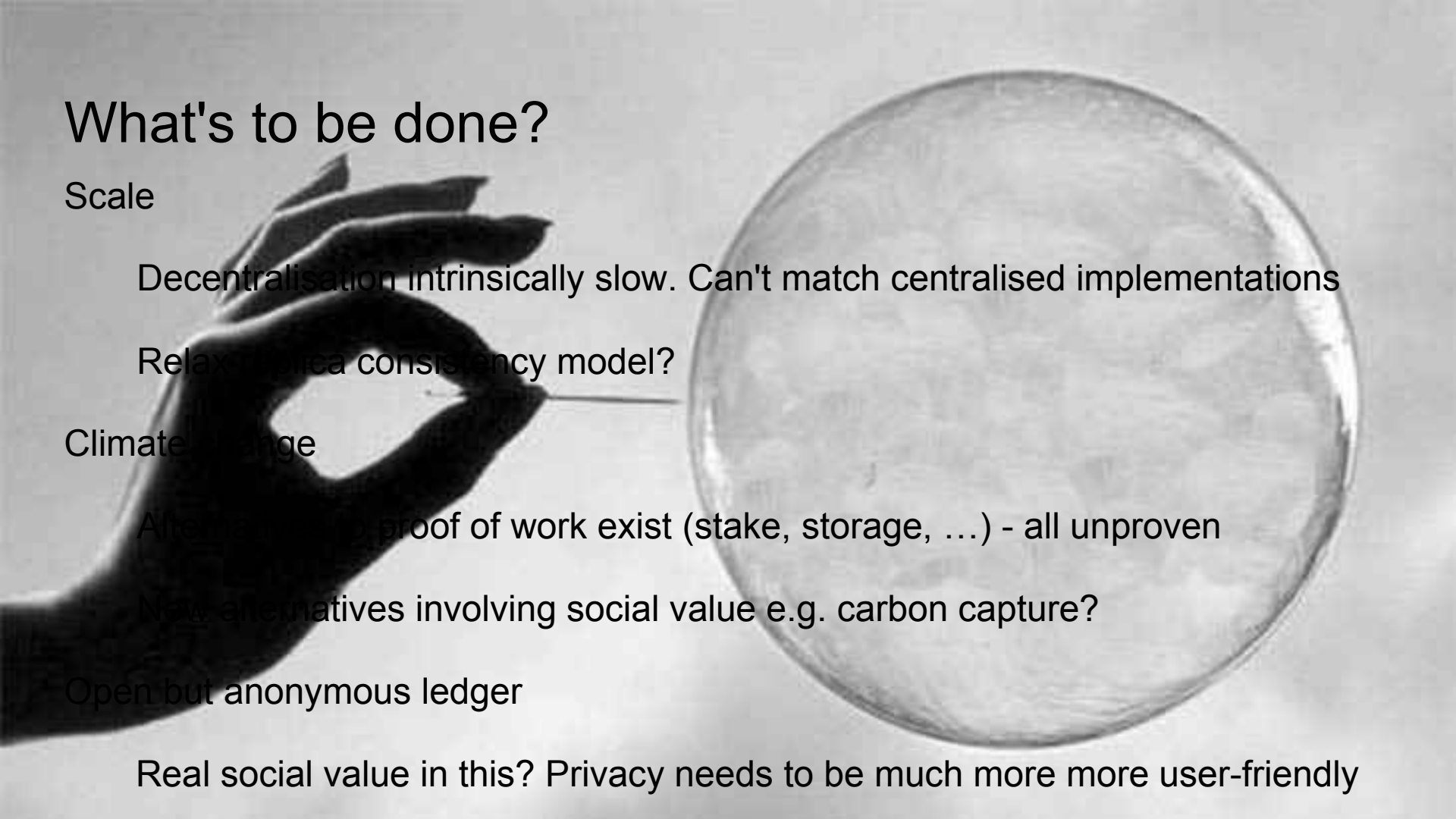
A decentralised algorithm - with new 'societal' elements

Suits anti-authority, Libertarian agenda

- 'Payments and governance by the people'

Experiment, needing not only computer science analysis but also:

- Economics
- Game theory
- Politics & other aspects of societal embedding (regulation, …)



What's to be done?

Scale

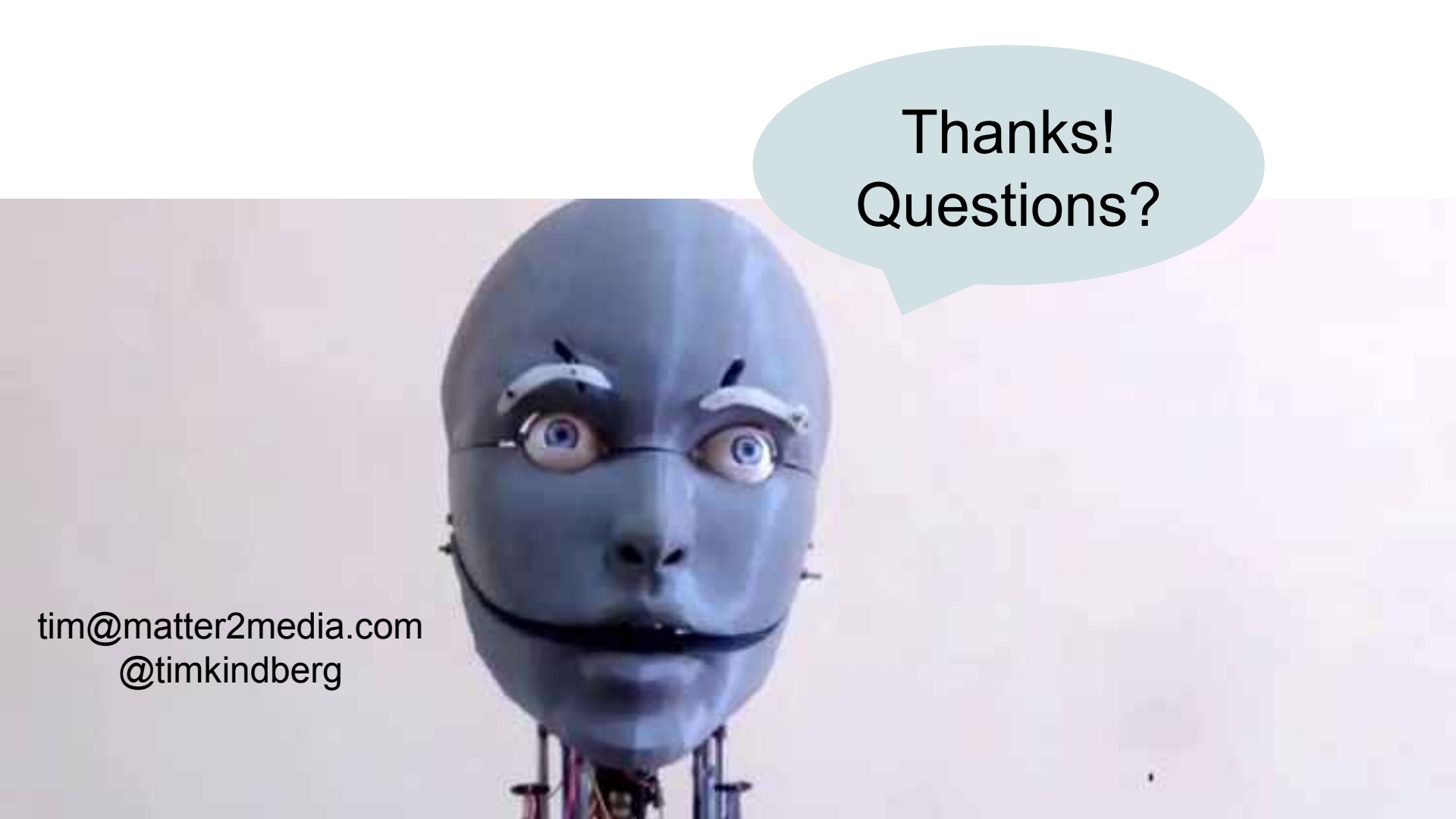
- Decentralisation intrinsically slow. Can't match centralised implementations
- Relax Byzantine consistency model?

Climate change

- Alternatives to proof of work exist (stake, storage, …) - all unproven
- New alternatives involving social value e.g. carbon capture?

Open but anonymous ledger

- Real social value in this? Privacy needs to be much more more user-friendly



tim@matter2media.com
@timkindberg

Smart contracts

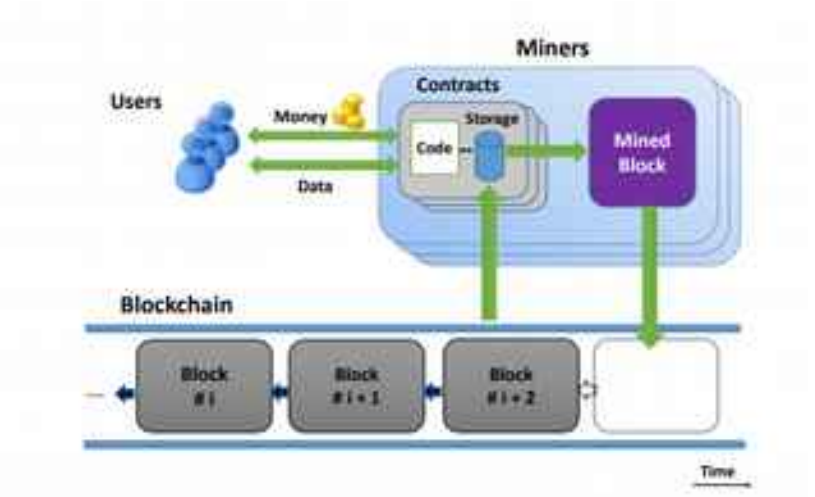
Gambling, 'cryptokitties', auctions, financial instruments, ...

Software and data stored in blockchain (Bitcoin, Ethereum)

Buggy implementation

Very hard code to write

Governance cannot be replaced by software!



Assumed knowledge (simplified)

For data *D*, **hash**(*D*) is a short derived value of fixed length acting as a proxy for *D*

given hash *H*, finding *D* such that hash(*D*) = *H* requires brute force

Public key cryptography (K_{secret}, K_{public})

owner uses K_{secret} to encrypt data, public uses K_{public} to decrypt it

A's **digital signature** for *D* is hash(*D*) encrypted with *A*'s secret key