Blockchain for Sceptics

Tim Kindberg

For Sceptics

Demystification of tech. Actual value? Problems?

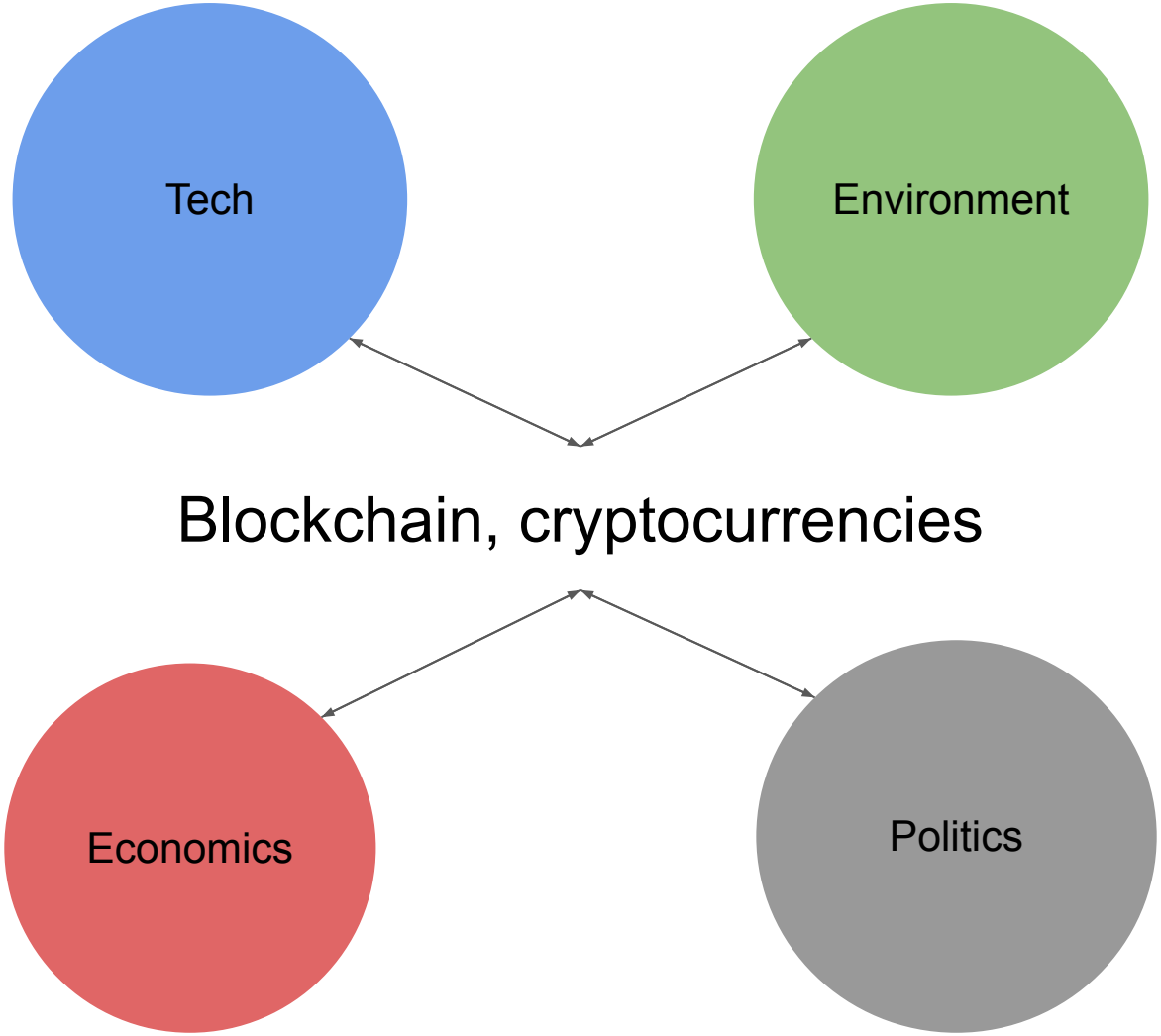
Questioning of agendas behind it

Creative response

Scepticism (evidence) vs cynicism (outlook)

Tradition in science, philosophy

Bitcoin & blockchain


Tech
Environment
Blockchain, cryptocurrencies
Economics
Politics


Serial number
Nominal value
Bank of England
AK47 900731
£5
Five Pounds
I have nothing to offer but blood, toil, tears and sweat
Sir Winston Churchill 1874-1965
AK47 900731
© THE GOVERNOR AND COMPANY OF THE BANK OF ENGLAND 2015

Goals for digital currency ("cryptocurrency")

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

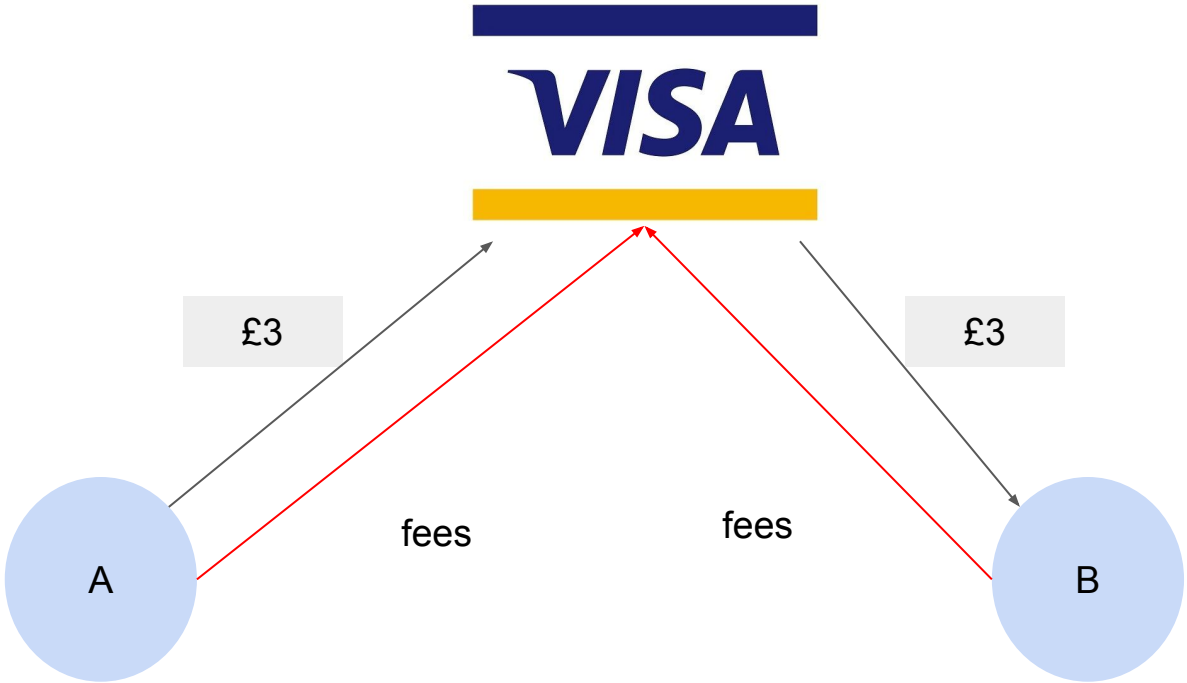
Decentralise transactions - no trusted third parties (gov't, financial institutions)

Low transaction fees

Pseudonymity / anonymity

Visa Transaction

A pays B £3



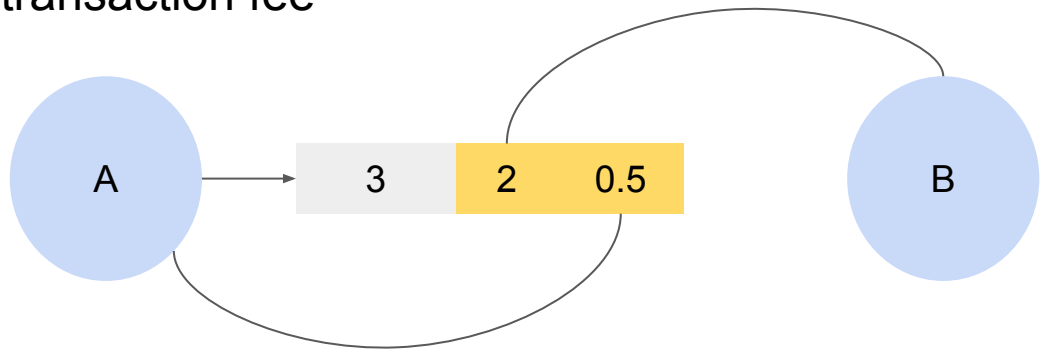
Bitcoin Transaction

Bitcoin: a digital currency realised through decentralised transactions

inputs are previous transactions paying bitcoins to *A*

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

Difference is a transaction fee

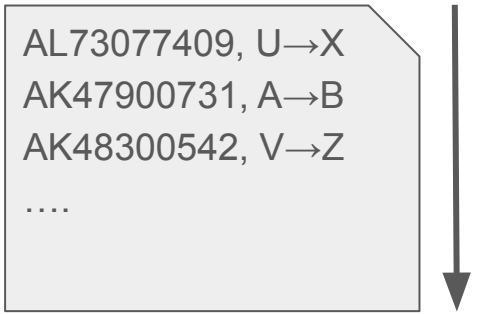


Digital currency, ledgers

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

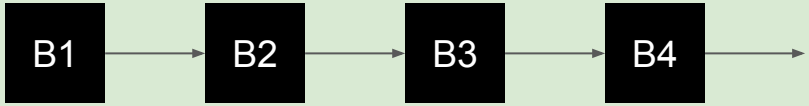
Prevent with a **Ledger**:

- Append-only, immutable, public record of transactions
- Whichever appears first for a given coin from A 'wins'



Ledger

Blockchain as data structure



Digital equivalent of pages in a physical ledger

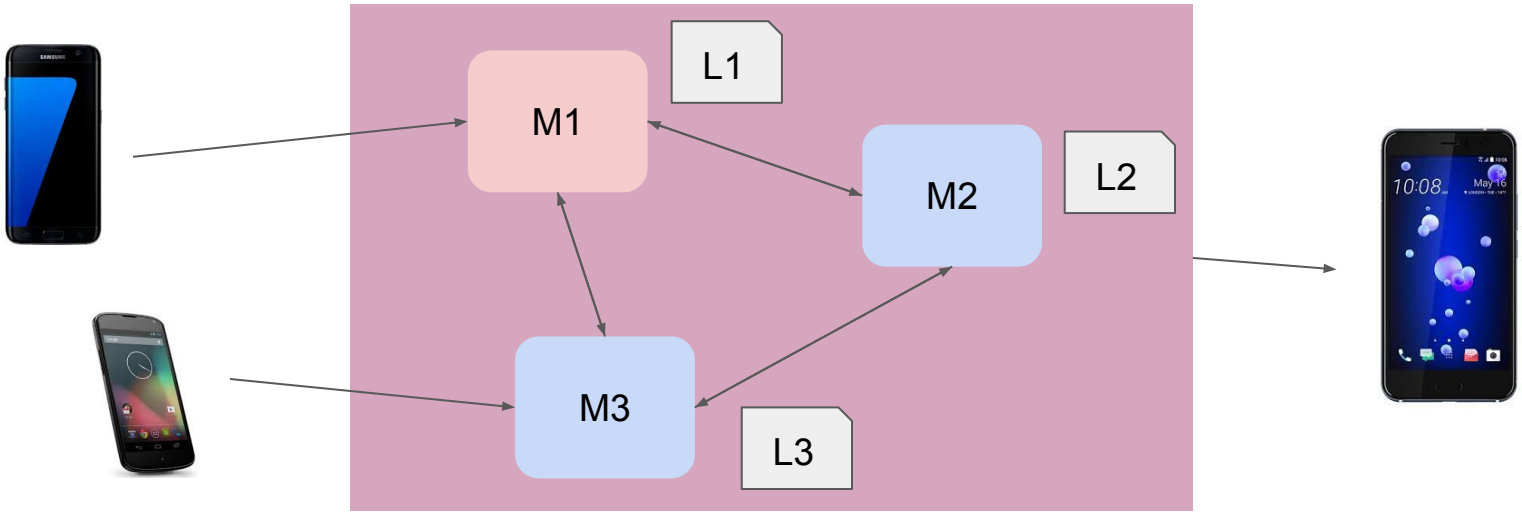
Each block contains records, like a page in a ledger

Evident if change/delete/reorder records/blocks (cryptographically linked)

Public, but identifiers anonymised (Jo Smith → 341878234730)

E.g. bitcoin transactions, land registry transactions

Blockchain as product of distributed consensus

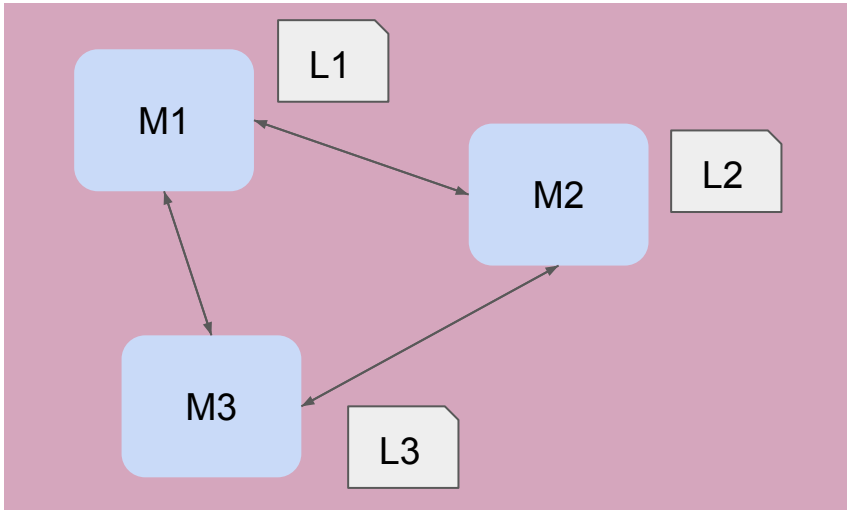


Collection of **miners** (can be anyone), instead of centralised authority

Add blocks of transactions to ledger

Forward transactions and new blocks to other miners

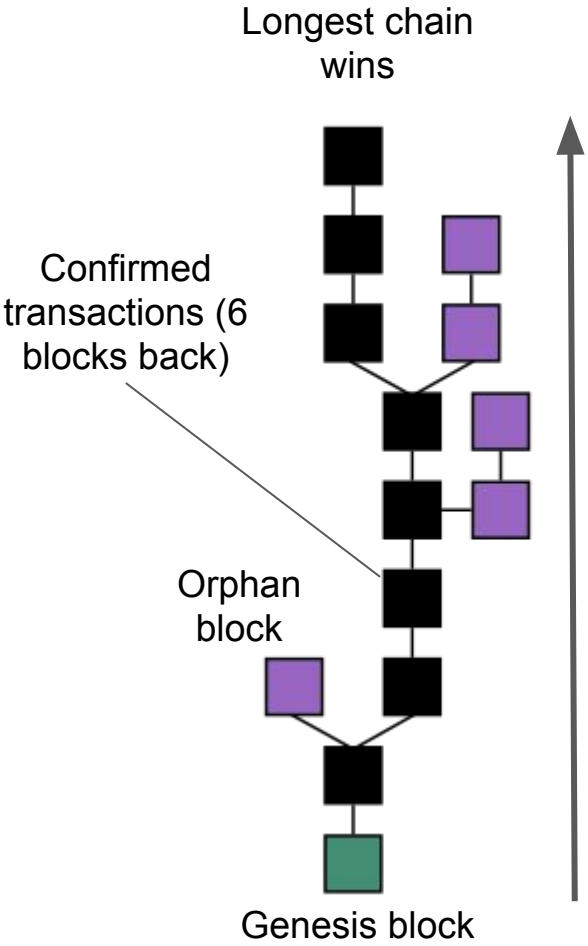
Distributed Consensus



No central authority

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* believes has *A*'s money, and so does *C*

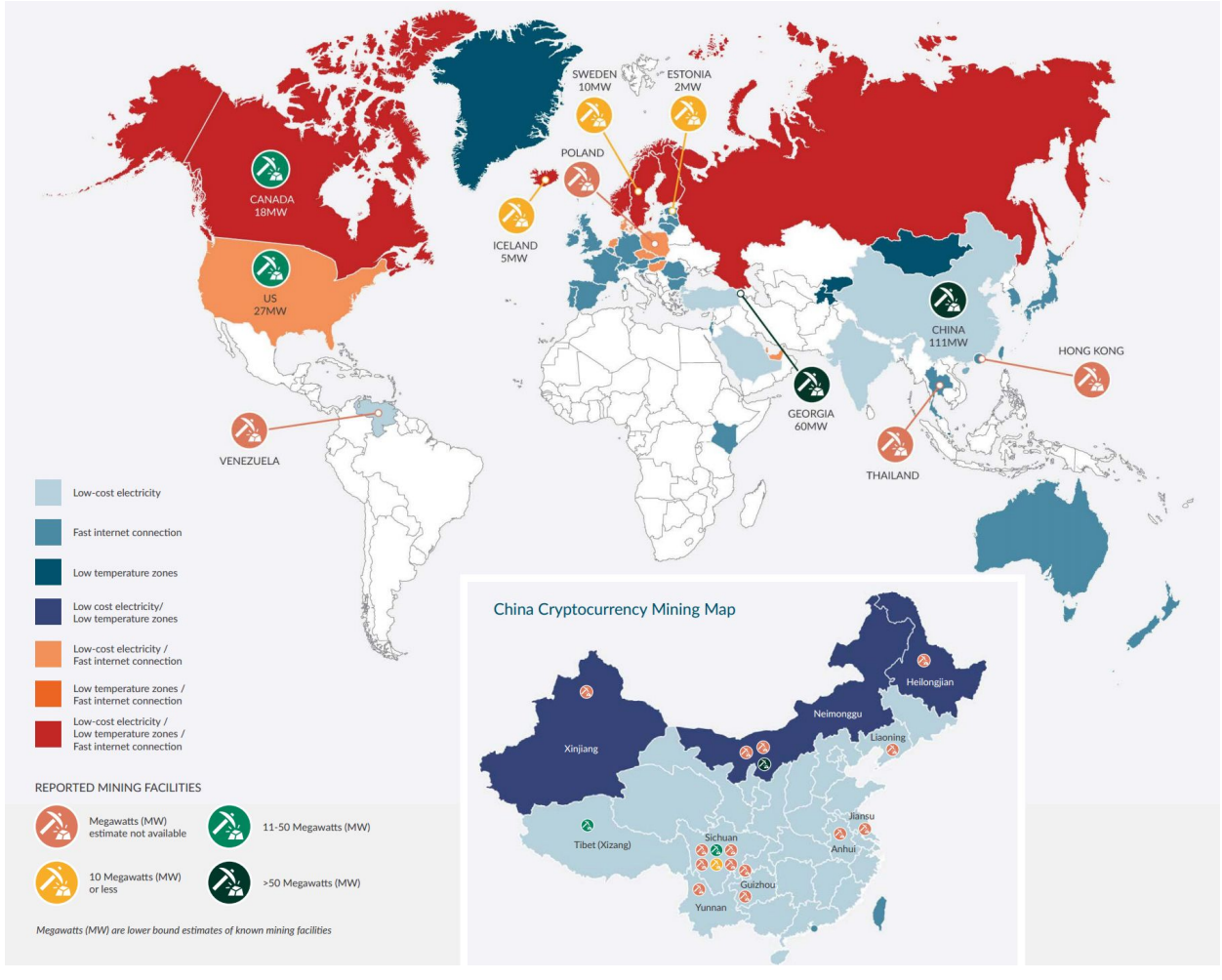
Incentivise good behaviour: if *M* 'mines' a new block, reward with new bitcoins - on top of transaction fees

Proof of work: significant computation to mine a block (hence name)

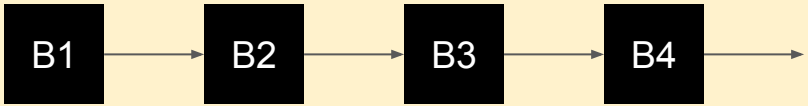
Find n for block B such that hash(n + B) < d (difficulty)

If compute power of good guys > 50% of total, bad guys can't succeed

Proof of Work


SWEDEN
10MW
ESTONIA
2MW
POLAND
ICELAND
5MW
CANADA
18MW
US
27MW
CHINA
111MW
HONG KONG
GEORGIA
60MW
THAILAND
VENEZUELA
Low-cost electricity
Fast internet connection
Low temperature zones
Low cost electricity/
Low temperature zones
Low-cost electricity /
Fast internet connection
Low temperature zones /
Fast internet connection
Low-cost electricity /
Low temperature zones /
Fast internet connection
REPORTED MINING FACILITIES
Megawatts (MW)
estimate not available
11-50 Megawatts (MW)
10 Megawatts (MW)
or less
>50 Megawatts (MW)
Megawatts (MW) are lower bound estimates of known mining facilities
China Cryptocurrency Mining Map
Heilongjian
Neimonggu
Liaoning
Xinjiang
Jiansu
Tibet (Xizang)
Sichuan
Anhui
Guizhou
Yunnan

Actual / plausible / implausible blockchain applications



Bitcoin transactions

Gambling

Land registry transactions

Voting

Medical records

Northern Ireland/Eire trade (Brexit)

Blockchain for International Development

MERL Tech report

"Blockchain is a type of **distributed database** that creates a **nearly unalterable record** of cryptographically secure **peer-to-peer transactions** without a **central, trusted administrator**. While it was originally designed for digital financial transactions, it is also being applied to a wide variety of interventions, including **land registries**, **humanitarian aid disbursement in refugee camps**, and **evidence-driven education subsidies**. International development actors, including government agencies, multilateral organizations, and think tanks, are looking at blockchain to improve effectiveness or efficiency in their work."

Blockchain for International Development

"We documented **43 blockchain use-cases** through internet searches, most of which were described with glowing claims like “operational costs… reduced up to 90%,” or with the assurance of “accurate and secure data capture and storage.” We found a **proliferation of press releases, white papers, and persuasively written articles**. However, we found **no documentation or evidence of the results** blockchain was purported to have achieved in these claims. We also **did not find lessons learned or practical insights**, as are available for other technologies in development."

Questions

Is Blockchain a database? (Nope) Did you need a database? (Yep)

Does Blockchain consensus scale? (No)

Are Blockchain transaction costs low - cup of coffee? (Not under load)

Preserves anonymity? (Don't count on it)

Is Blockchain provably correct? (Hmmmm) Secure? (No - exchanges)

Does Blockchain eliminate trusted third parties? (No - changes trust landscape)

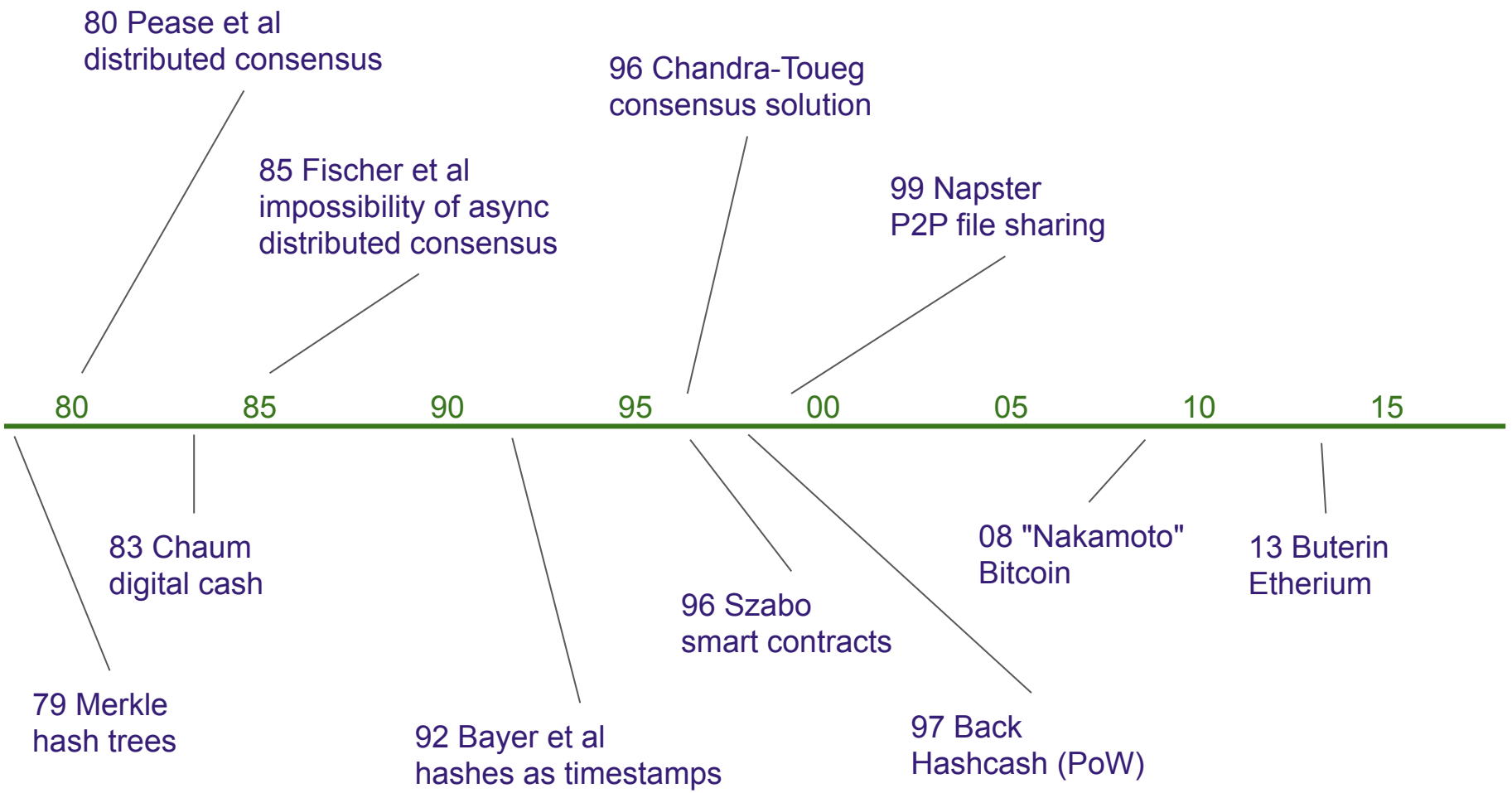
Is Blockchain fit for an era of global warming? (No - it's shameful)

Reflections

It's early days, right?

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

It's hard. And a socially embedded protocol is harder

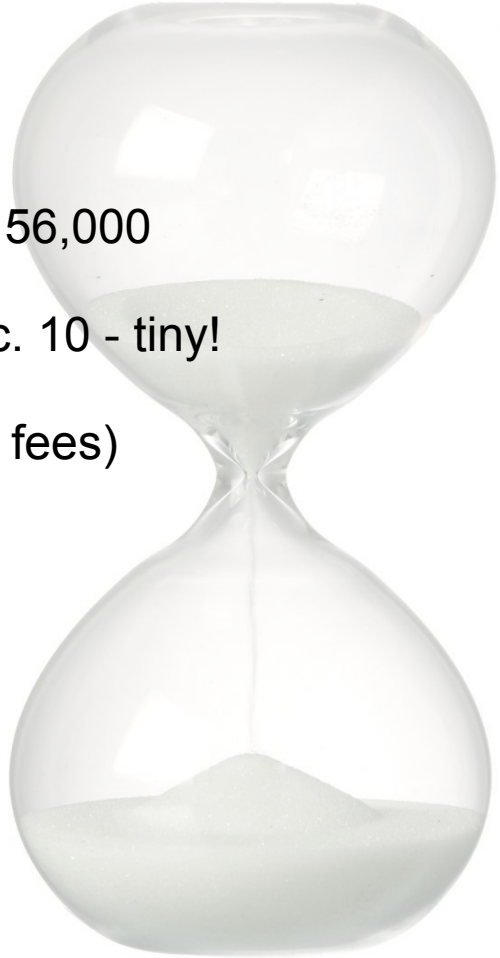

80 Pease et al
distributed consensus
85 Fischer et al
impossibility of async
distributed consensus
96 Chandra-Toueg
consensus solution
99 Napster
P2P file sharing
80
85
90
95
00
05
10
15
79 Merkle
hash trees
83 Chaum
digital cash
92 Bayer et al
hashes as timestamps
96 Szabo
smart contracts
97 Back
Hashcash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

Numbers (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)



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

Bitcoin blockchain size: c. 190GB

Block creation rate: 1 per 10 minutes (normative)

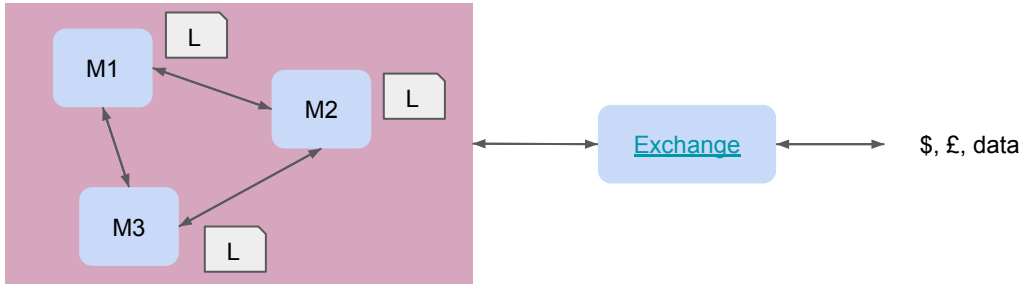
Mining difficulty adjusted every 2016 blocks

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

Third parties: exchanges, miners, developers, ...



Decentralisation (no central authority) helps against failure

Trust is one of the bases of civilisation. Hand in hand with accountability

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

Blockchain ecosystems (devs, 'leaders', advocates, …)

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

Smart contracts

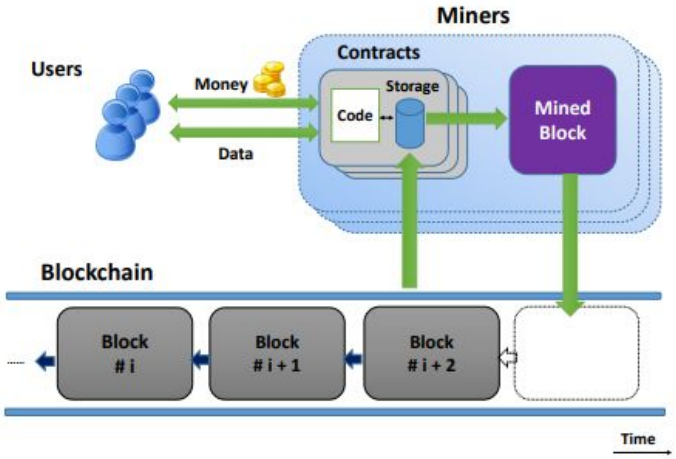
Gambling, 'cryptokitties', auctions, financial instruments, ...

Software and data stored in blockchain (Bitcoin, Ethereum)

Buggy implementation

Very hard code to write

Governance cannot be replaced by software!



What's new about blockchain?

A decentralised algorithm - with new 'societal' elements

Suits anti-authority, libertarian/anarchist agenda

An interesting experiment. Requires not only computer science 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 consistency model?

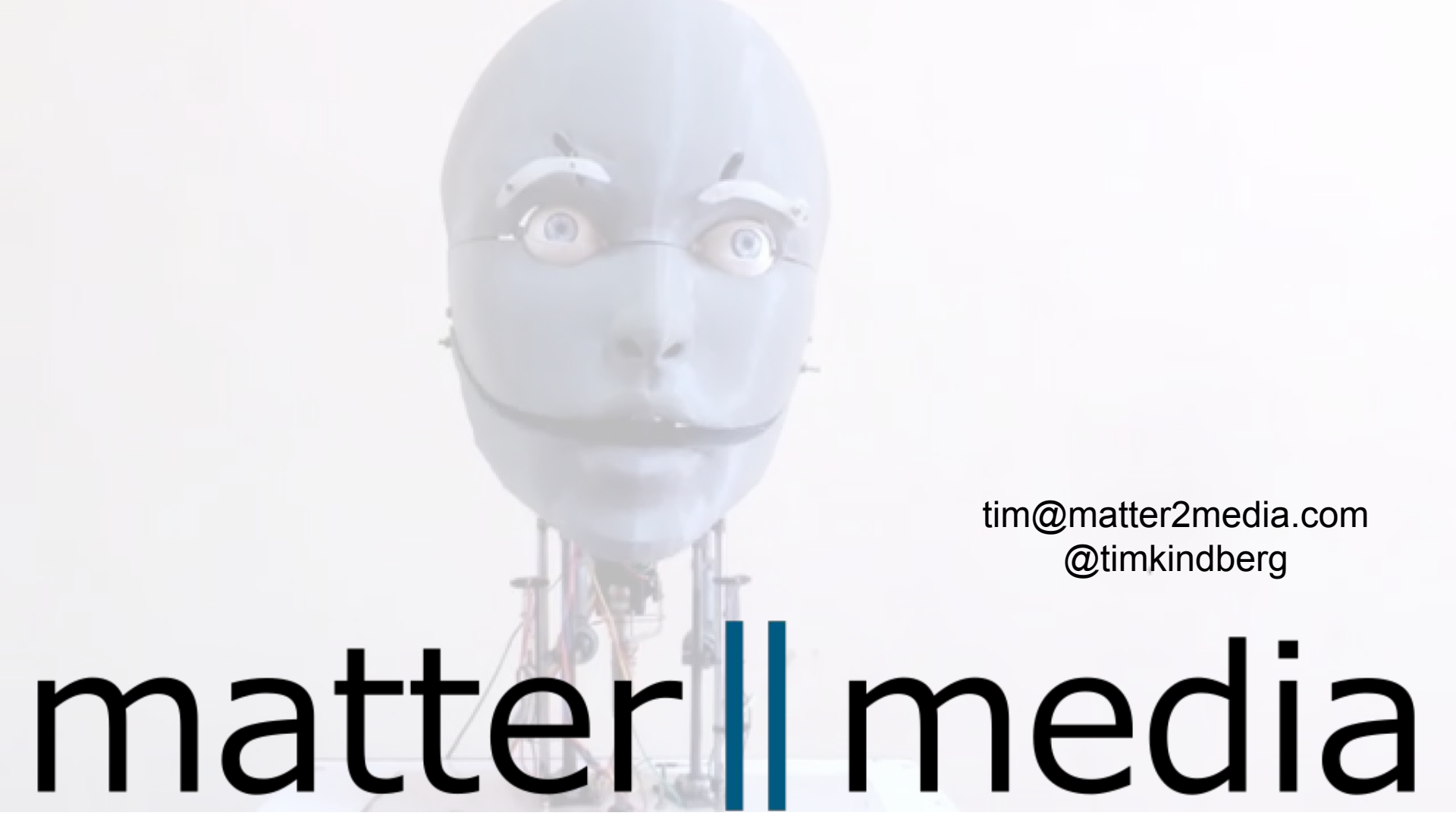
Climate change

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 user-friendly



tim@matter2media.com
@timkindberg

matter || media