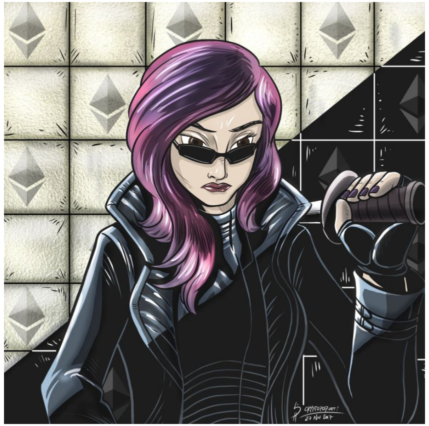
Amsterdam
2018

CLOSING KEYNOTE

Security is what we make of it: blockchain & beyond

@AmberBaldet | #HITB2018AMS



© Hello Louis, cryptopop.net

$whois **Amber Baldet**

Previously:

- ➔ Executive Director, JPMorgan (Blockchain Program Lead)
- ➔ Chair, Financial Industry Working Group, Enterprise Ethereum Alliance

Currently:

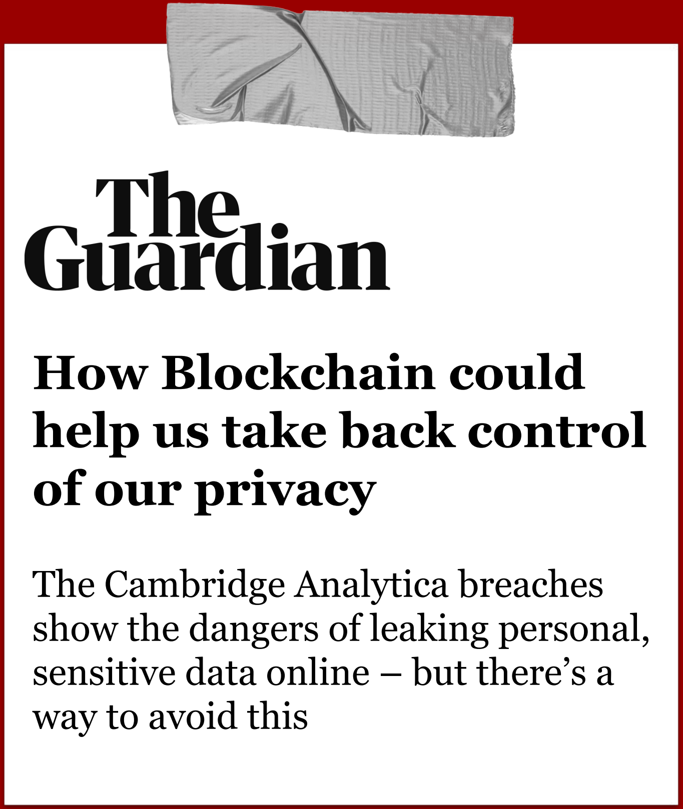
- ➔ Unemployed

Lectures, panels, etc:

- ➔ Defcon, Empire Hacking, SOURCE
- ➔ MIT Media Lab, Wharton, Duke, Harvard Business, NYU, Columbia
- ➔ Money 20/20, American Banker
- ➔ Hyperledger, EEA, Consensus, etc.

Likes: otters, memes, otter memes

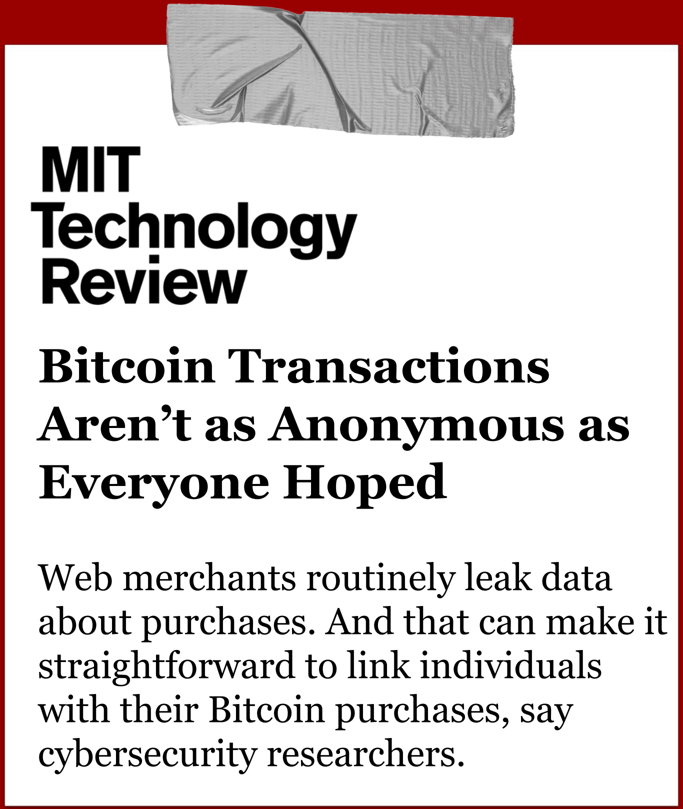
Dislikes: patriarchy



The Guardian

How Blockchain could help us take back control of our privacy

The Cambridge Analytica breaches show the dangers of leaking personal, sensitive data online – but there’s a way to avoid this

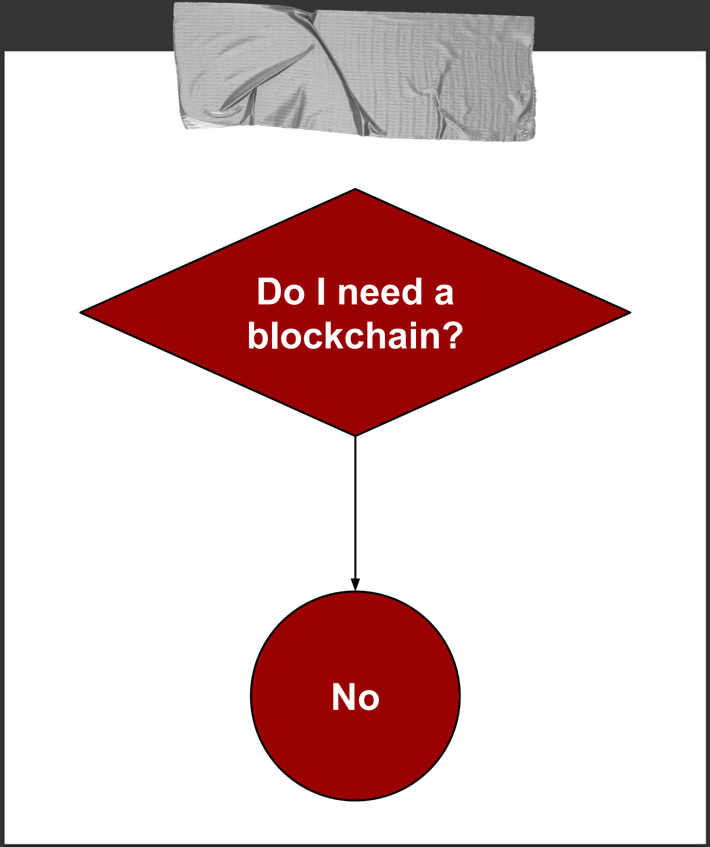


MIT Technology Review

Bitcoin Transactions Aren’t as Anonymous as Everyone Hoped

Web merchants routinely leak data about purchases. And that can make it straightforward to link individuals with their Bitcoin purchases, say cybersecurity researchers.

Hahaha, why don’t you just use a database?



Usually, you can

—

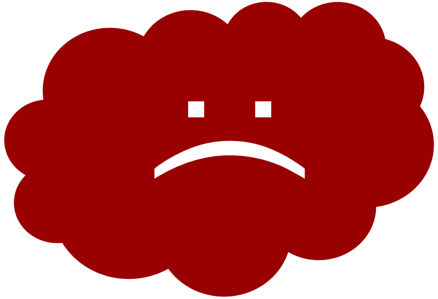
And sometimes, you could, but there are human reasons why centralized solutions failed to gain traction

—

And in other cases, we have, but they are inefficient, expensive and/or have failed disastrously

It’s not just a database…

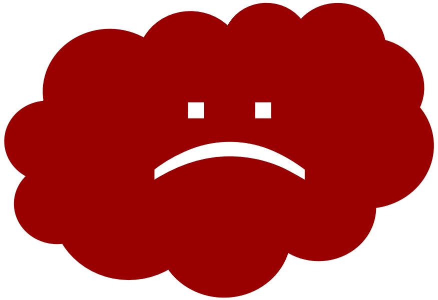
It's not just a database...



There is no cloud

It's just someone else's computer

It’s not just a database... it’s worse

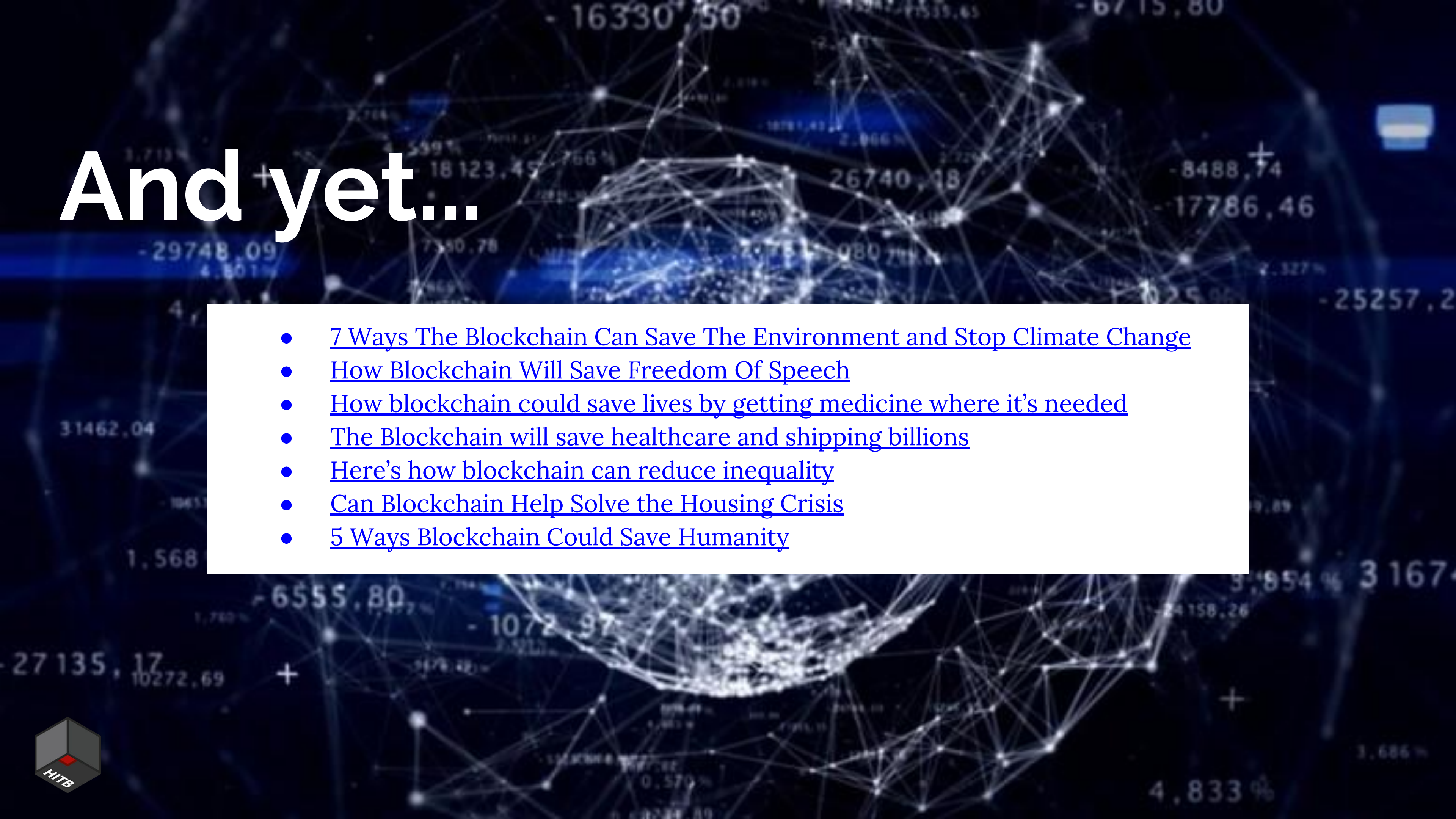


There is no cloud

It’s just someone else’s computer

There is no blockchain

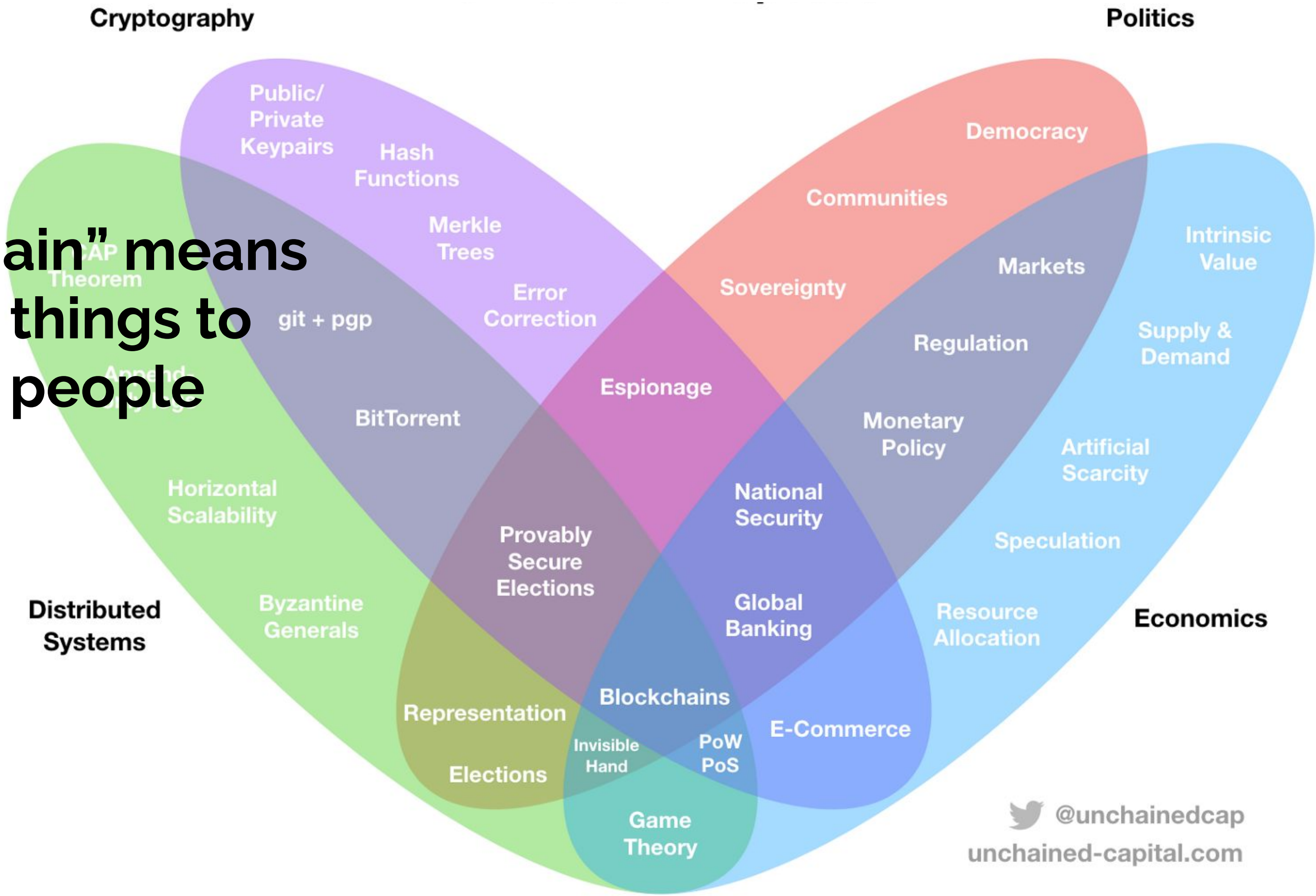
It’s just all of our computers



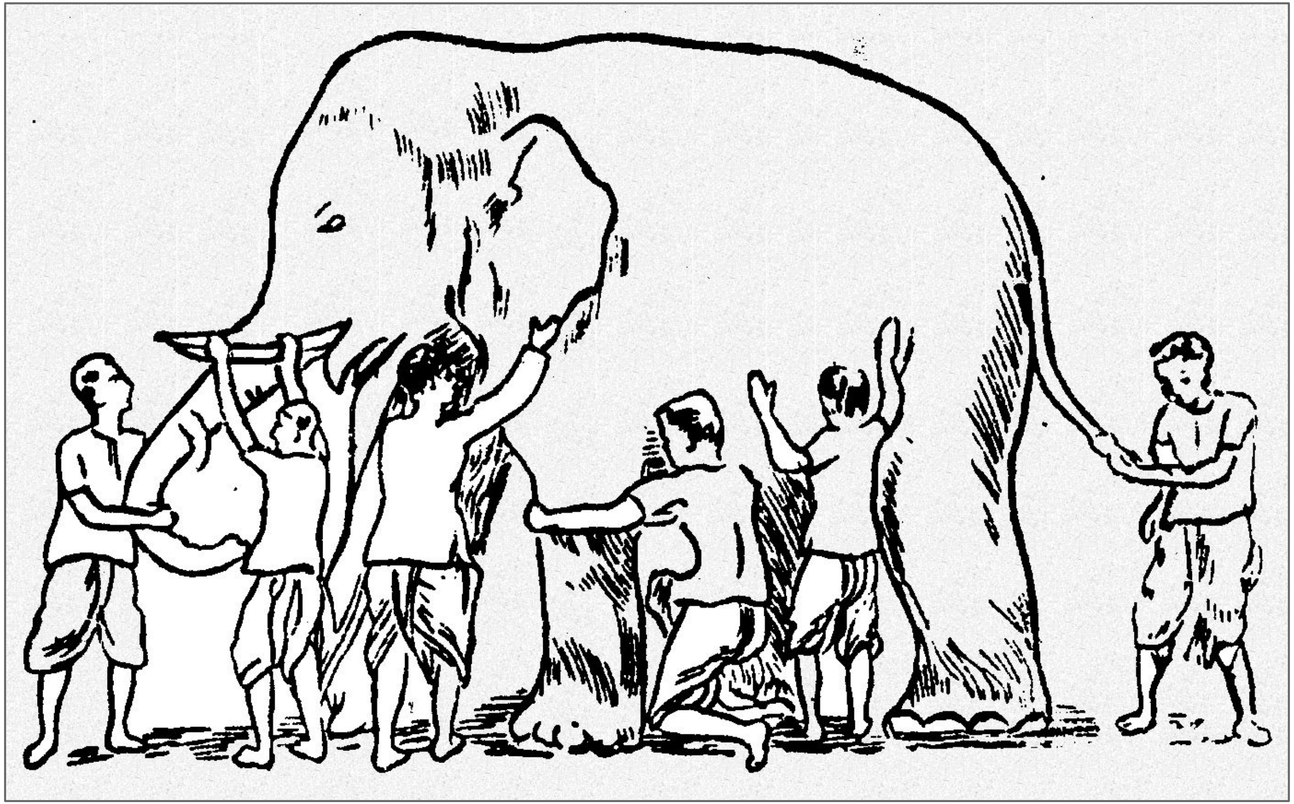
And yet...

- 7 Ways The Blockchain Can Save The Environment and Stop Climate Change
- How Blockchain Will Save Freedom Of Speech
- How blockchain could save lives by getting medicine where it’s needed
- The Blockchain will save healthcare and shipping billions
- Here’s how blockchain can reduce inequality
- Can Blockchain Help Solve the Housing Crisis
- 5 Ways Blockchain Could Save Humanity

“Blockchain” means different things to different people



Maybe try listening once in a while?



Businesses are experimenting

Distributed Database:

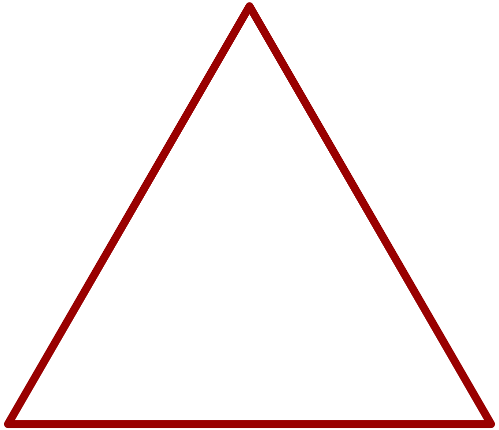
- ➔ Closed, single operator
- ➔ Trust among nodes
- ➔ Fast, capable of strong consistency
- ➔ Store of mutable state
- ➔ Resiliency & DR assumptions

Mutualized Infrastructure

Public Blockchain:

- ➔ Open, multiple operators
- ➔ Trustless, censorship resistant
- ➔ Slow, eventually consistent
- ➔ Log of state transitions
- ➔ Antifragile

Choose two:



Accessible
(Open)

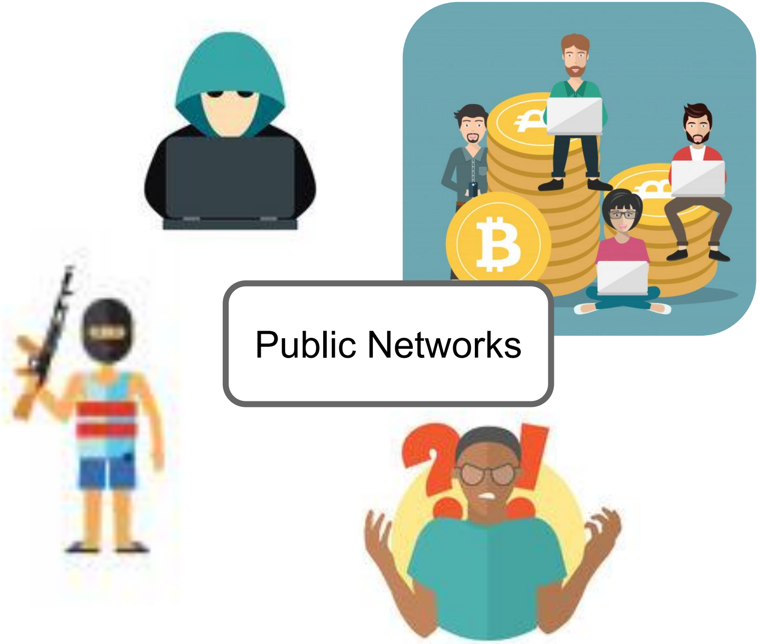
Flexible,
Resilient,
Performant

Confidential
& Secure

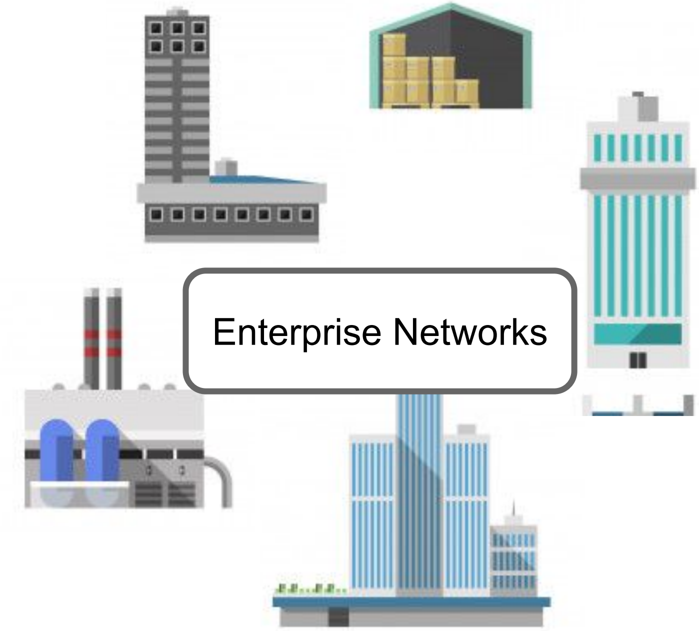
Business concerns

- ➔ Data privacy
- ➔ Compliance
- ➔ Governance
- ➔ Dispute resolution
- ➔ Performance
- ➔ Settlement finality
- ➔ Resilience

Isolated networks

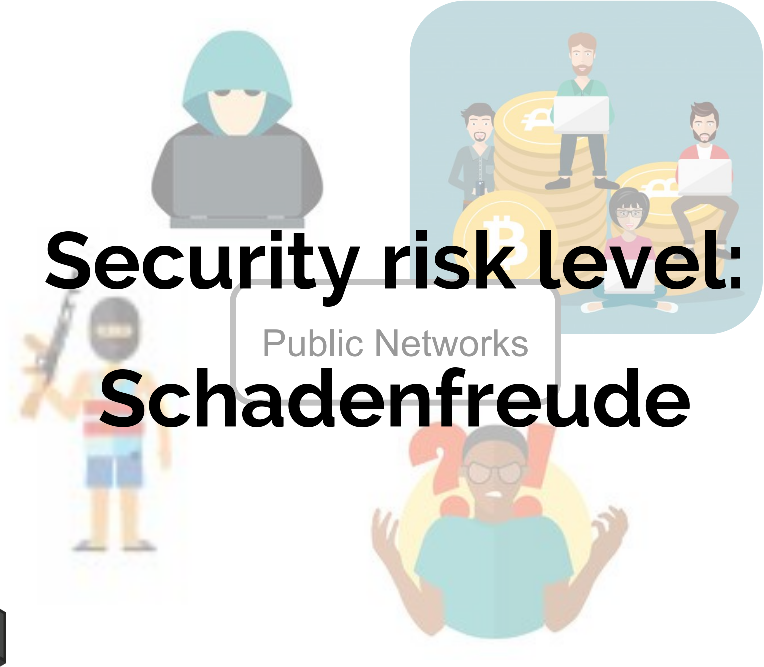


Public Networks



Enterprise Networks

Isolated networks



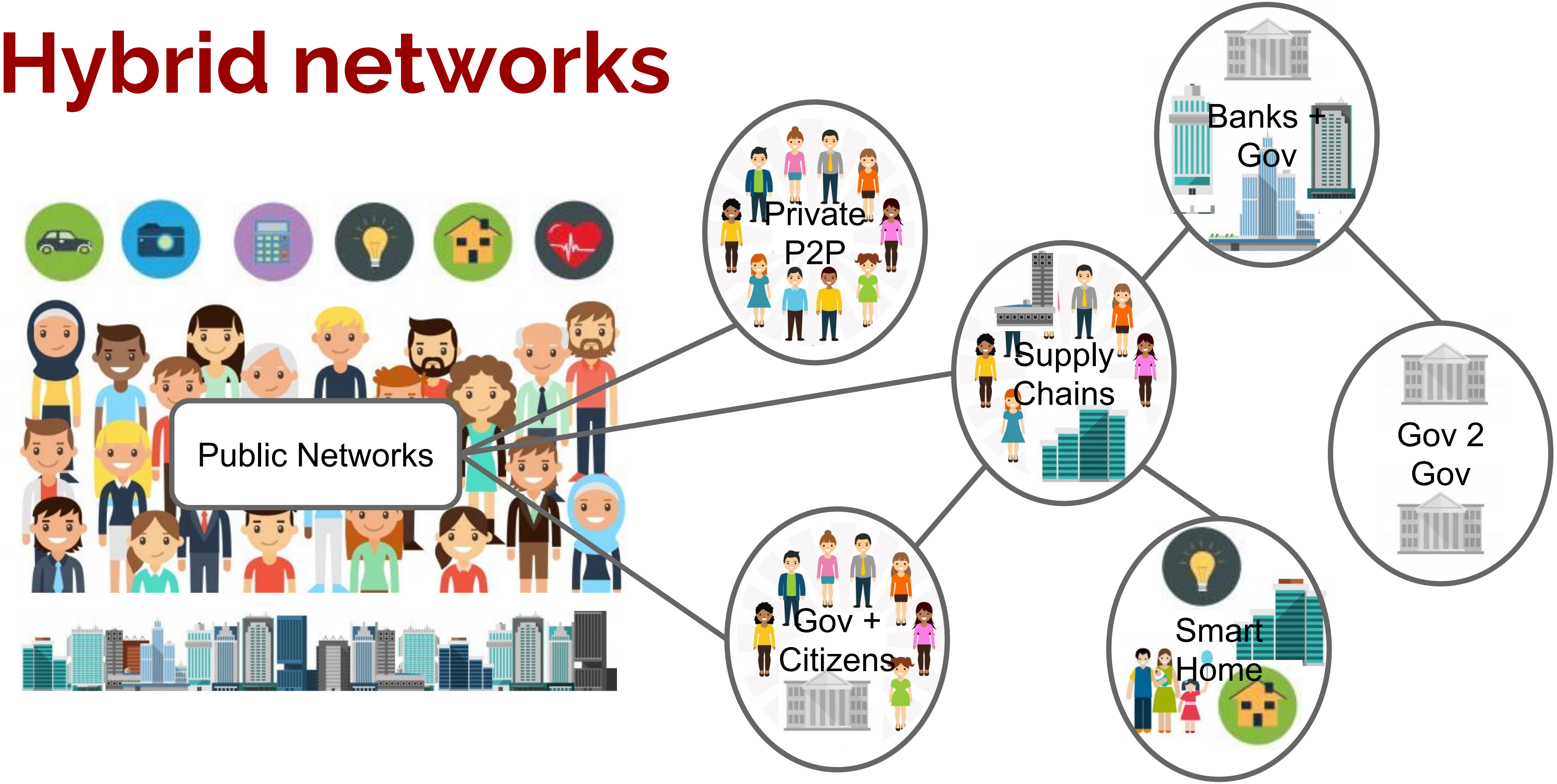
Security risk level:

Schadenfreude

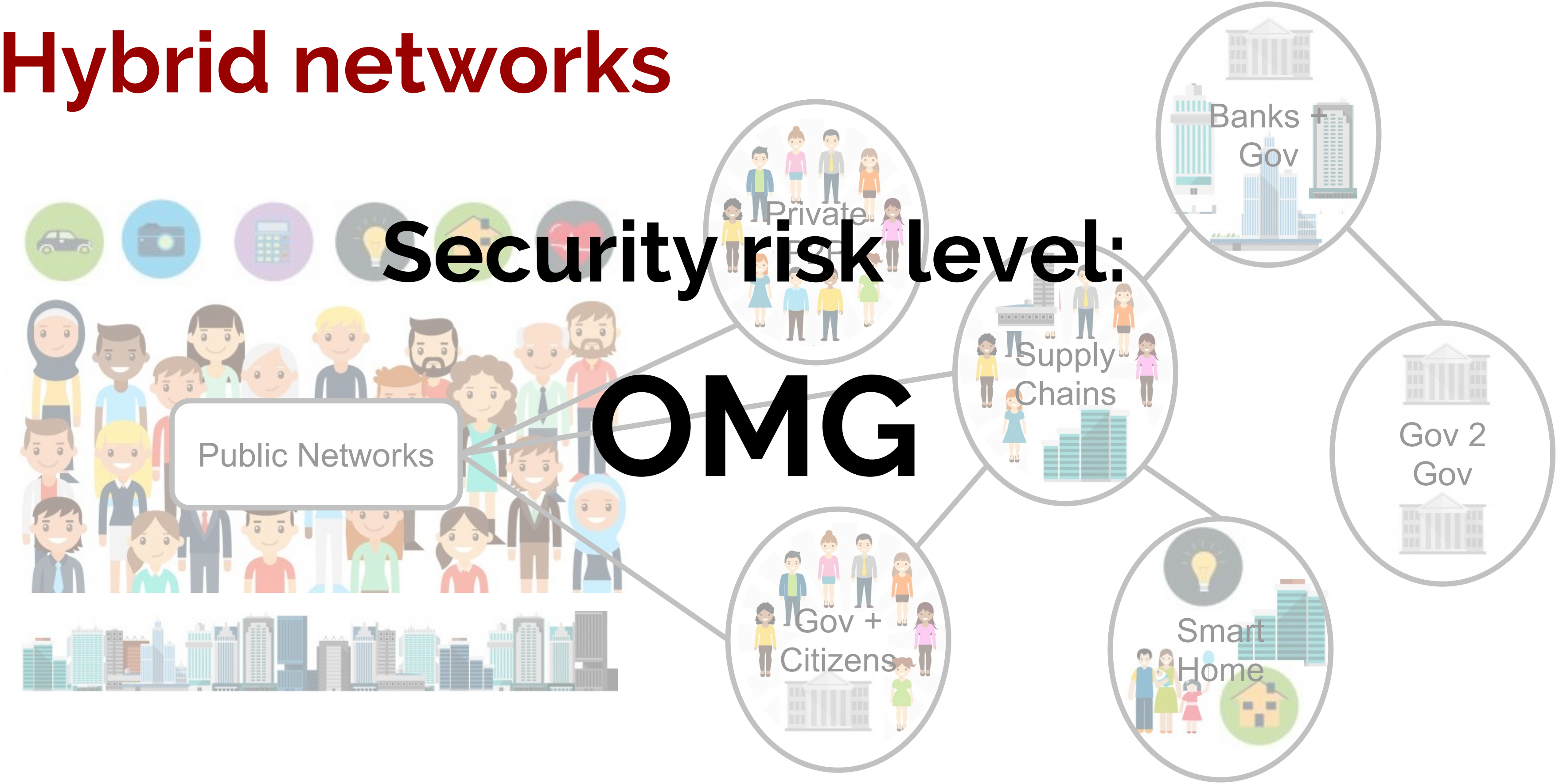
Security risk level:

Boring

Hybrid networks

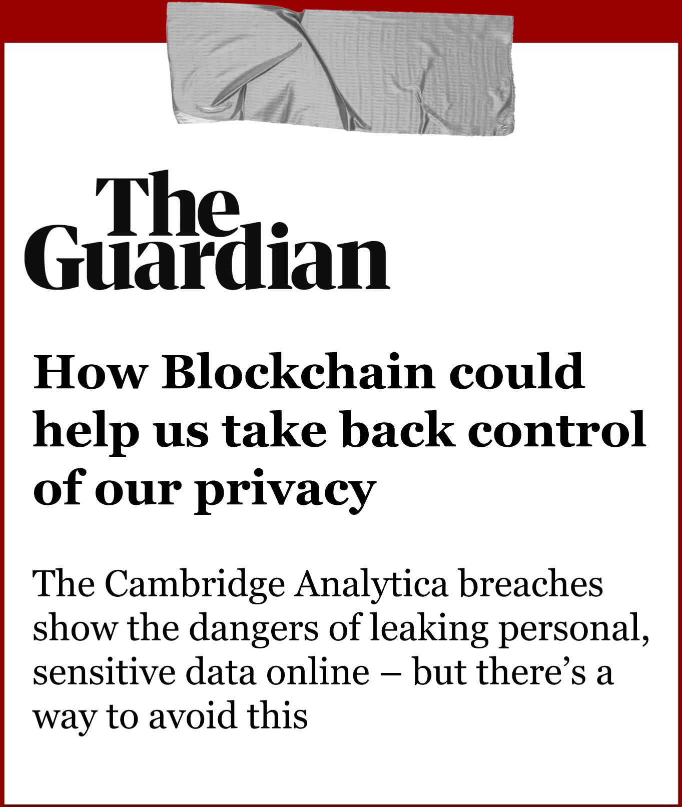


Hybrid networks



Security risk level:

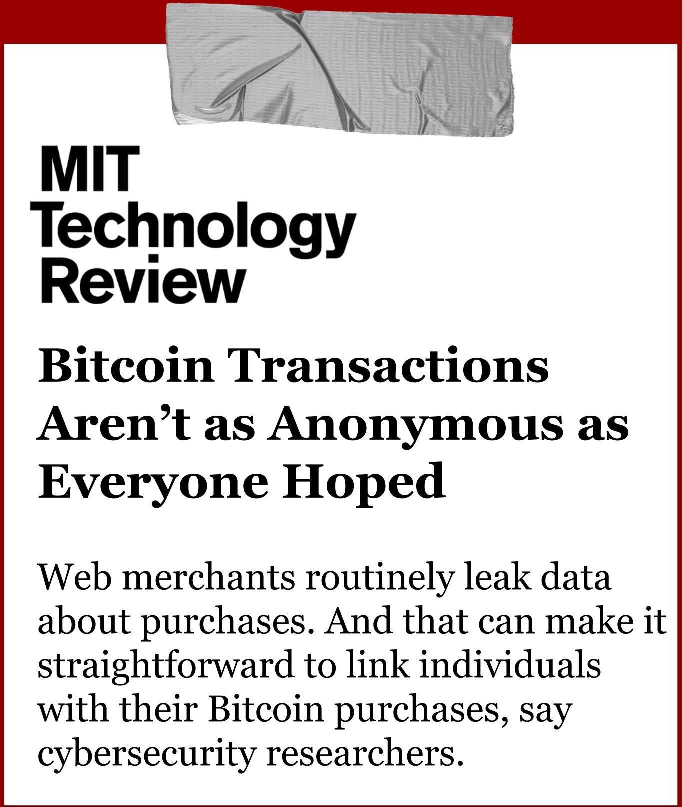
OMG



The Guardian

How Blockchain could help us take back control of our privacy

The Cambridge Analytica breaches show the dangers of leaking personal, sensitive data online – but there's a way to avoid this



MIT Technology Review

Bitcoin Transactions Aren't as Anonymous as Everyone Hoped

Web merchants routinely leak data about purchases. And that can make it straightforward to link individuals with their Bitcoin purchases, say cybersecurity researchers.

The future is coming…

What will it look like?

Blockchain + IoT + AI = Skynet

(and so many consulting white papers)

Your scientists were so preoccupied with whether
or not they could that they didn't stop to think if they should.

China

Russia

Venezuela

Next-gen encryption wars

Public blockchains are world readable data lakes

Increasingly, the anonymity of a part depends on the motivations & operational security actions of the whole

Businesses need privacy

Share primary records without

- ➔ surrendering information ownership to third parties
- ➔ creating centralized data lakes

Transition from a perimeter network security model to record level security

Drive adoption of significantly stronger encryption and data privacy standards

> “One particularly interesting partnership to highlight is between Ethereum, Zcash, and innovators at JPMorgan.”

-Peter Van Valkenberg,
CoinCenter Director of Research
Testimony to US House Energy & Commerce Committee, 2017

Businesses need privacy

Share primary records without

- ➔ surrendering information ownership to third parties
- ➔ creating centralized data lakes

Transition from a perimeter network security model to record level security

Drive adoption of significantly stronger encryption and data privacy standards

And real people do, too!

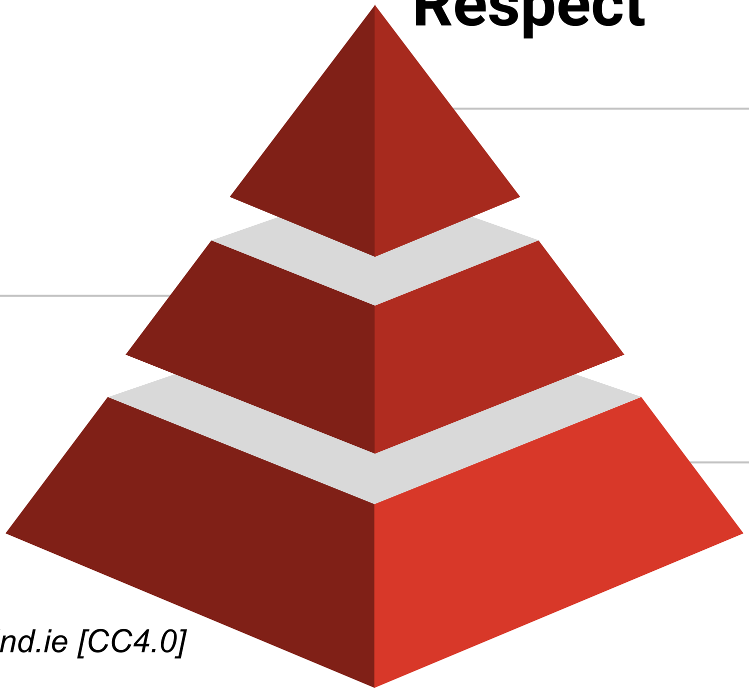
Take your records with you, forever

- ➔ Move records between doctors
- ➔ Prevent diploma fraud
- ➔ Prove your credentials & credit history when you move countries

Monetize your data

- ➔ Opt in sharing of personal data with enforceable licensing
- ➔ Microtransactions via cryptocurrency
- ➔ Secure hardware can bring algos to your data rather than sending data out

Ethical Design



Respect

1 **Human Experience**

Delightful

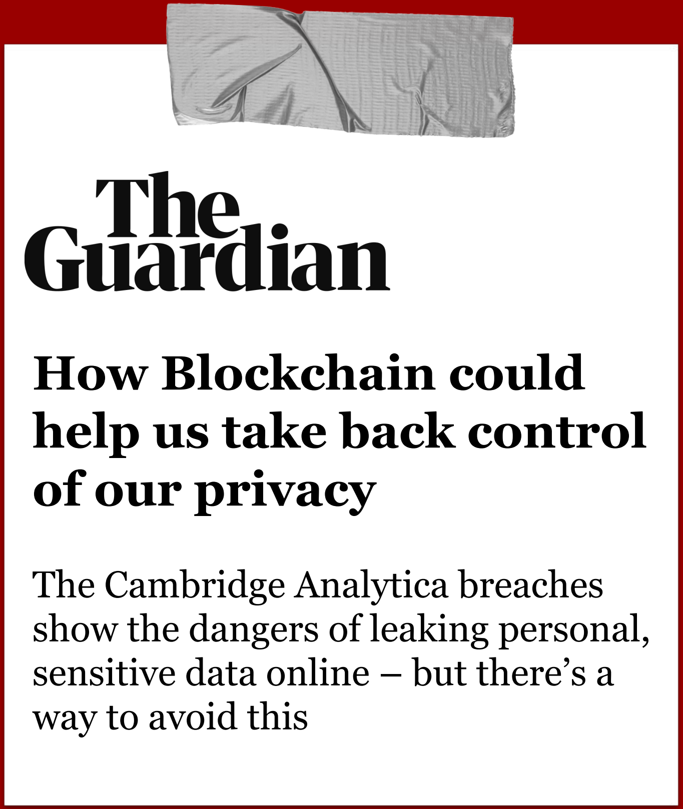
2 **Human Effort**

Functional, convenient, & reliable

3 **Human Rights**

Decentralized, private, open, interoperable, accessible, secure, & sustainable

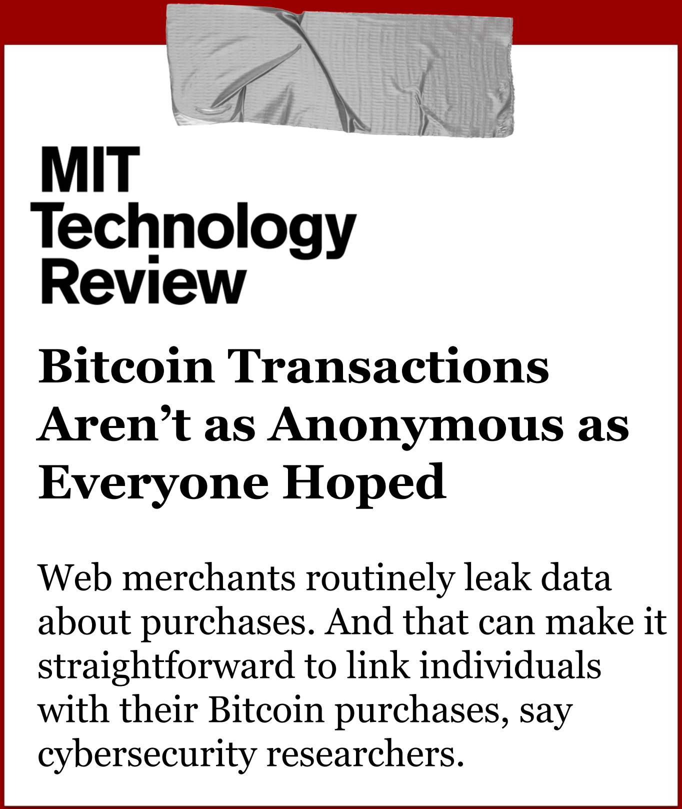
© ind.ie [CC4.0]



The Guardian

How Blockchain could help us take back control of our privacy

The Cambridge Analytica breaches show the dangers of leaking personal, sensitive data online – but there's a way to avoid this



MIT Technology Review

Bitcoin Transactions Aren't as Anonymous as Everyone Hoped

Web merchants routinely leak data about purchases. And that can make it straightforward to link individuals with their Bitcoin purchases, say cybersecurity researchers.

Smart contract testing is maturing

Analysis Tools:

- Manticore
- Echidna
- Ethersplay
- Mythril
- Porosity
- Solgraph
- solcheck
- SmartCheck
- Oyente
- 4byte.directory

Auditing Services:

- Open Zeppelin
- Trail of Bits
- Securify
- Hosho
- New Alchemy
- Authio

Otherwise, security be like ¯_(ツ)_/¯

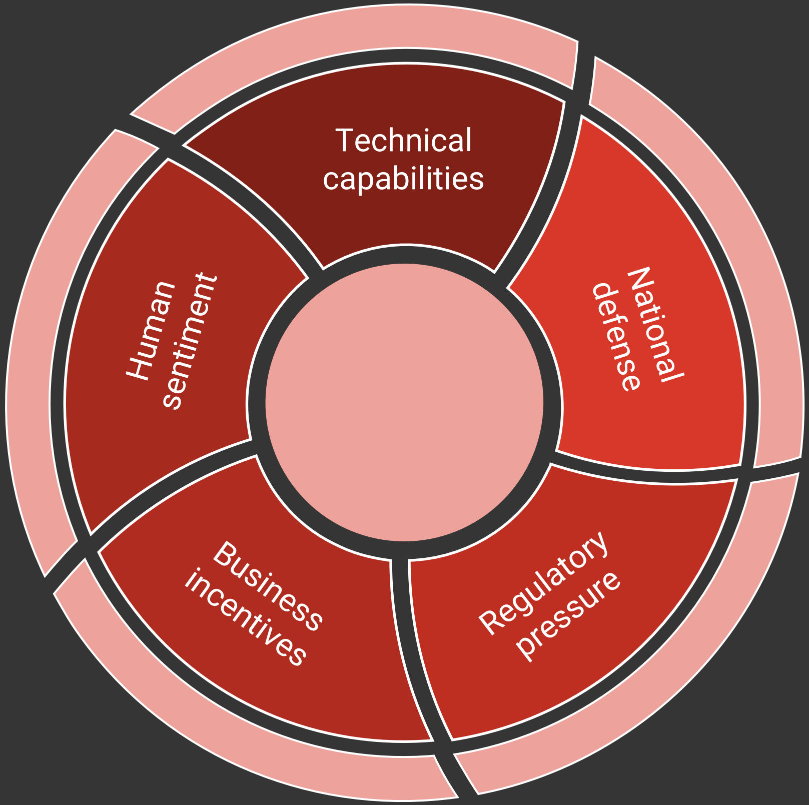
Public:

- Hacked exchanges?
- Compromised hardware?
- Fake donation scams?
- Literal 51% attacks?
- Non-mining consensus?
- Bespoke crypto schemes?
- “Faux decentralization”?
- Patch management?
- USABLE PRIVACY???

Permissioned:

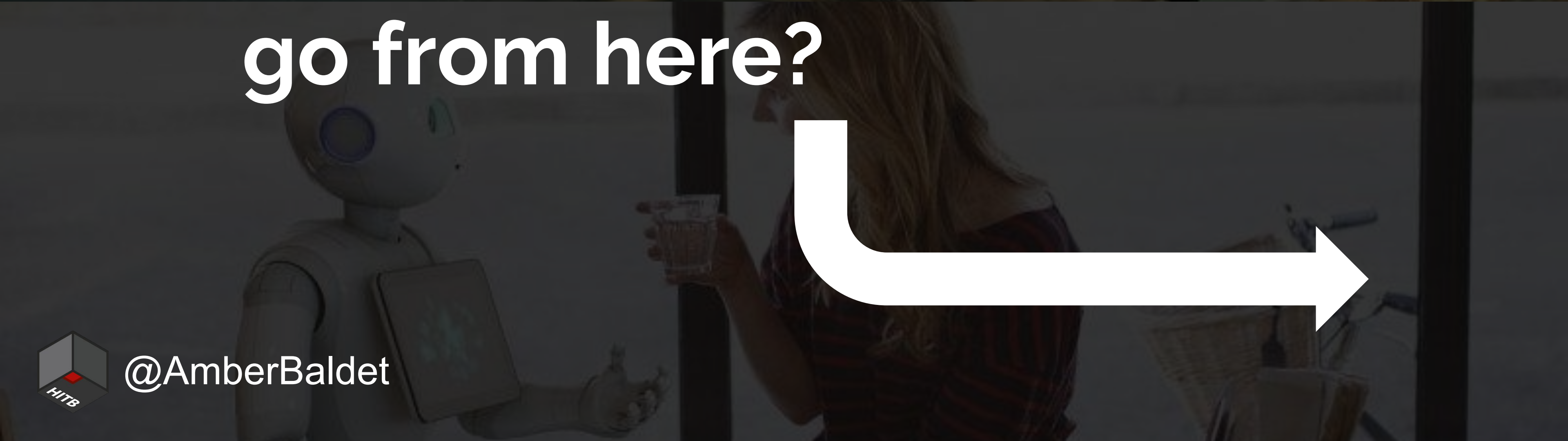
- Identity & Access mgmt?
- Secure hardware as panacea?
- Shared governance tools?
- Delegated cloud mgmt?
- Integration into existing risk management processes?
- Veracity of data oracles?
- Patch management?
- USABLE PRIVACY???

Hope...


Technical capabilities
National defense
Regulatory pressure
Business incentives
Human sentiment

But we need YOU

- Intrusion detection
- Red team
- Blue team
- Pentesting
- Risk & threat modeling
- CISO / CSO
- Applied cryptography
- NOC
- Cloud security
- AppDev
- QA
- DevOps
- UX
- Business Analyst
- Product Manager
- Political scientist
- Economist
- Defense



Where will we go from here?

@AmberBaldet