# Perspectives on blockchain and 5 things you shouldn't use blockchain for

Martin Gilje Jaatun

Adjunct Professor, UiS

Senior Scientist SINTEF

Co-chair, IEEE CS Special Technical Community on Blockchain

University of Stavanger

# First a comment on ICOs

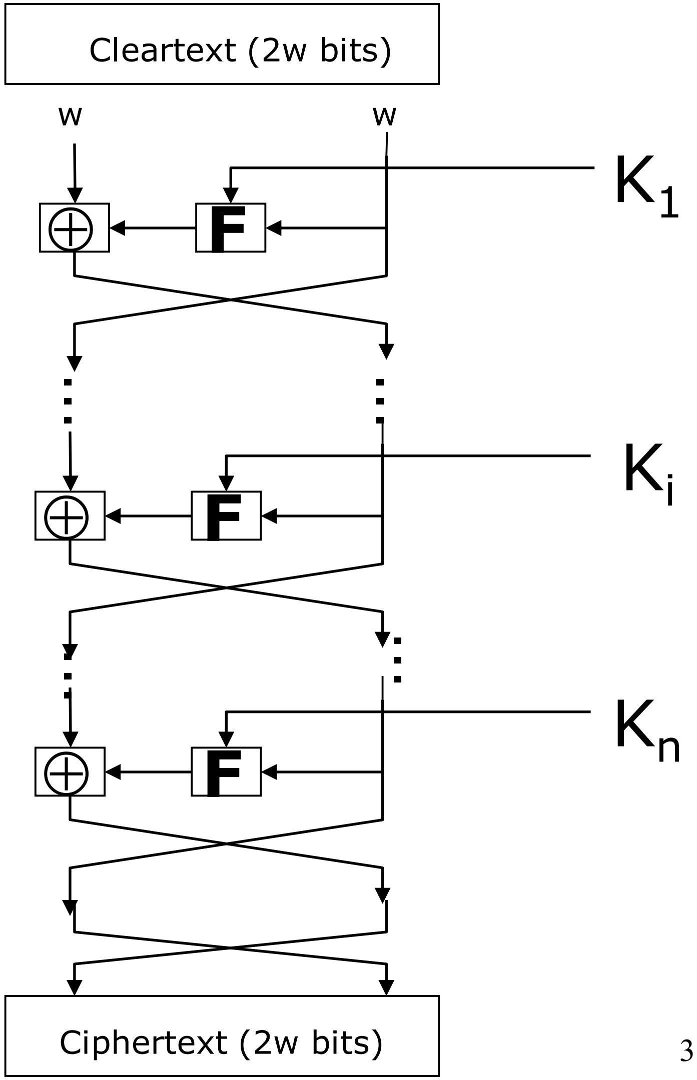
ICO = Initial Coin Offering

The "i" is optional

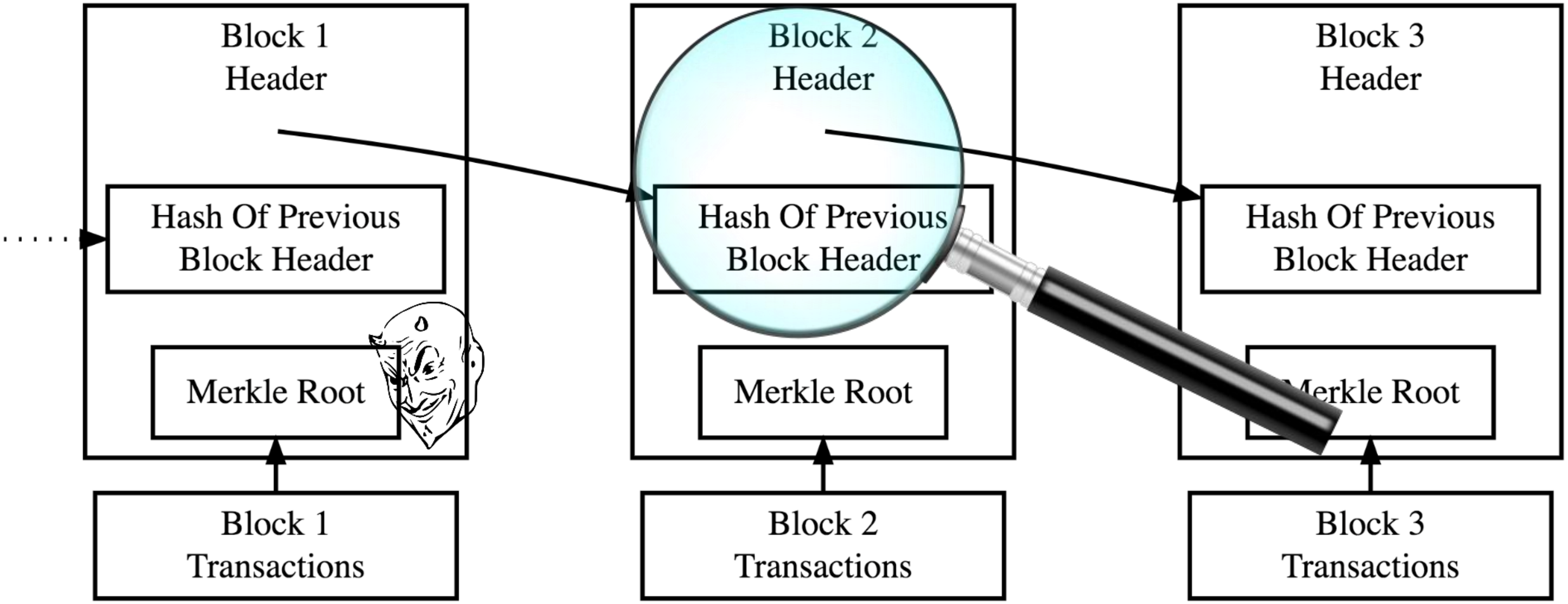
Credit: Prof. Roman Vitenberg, UiO

# What is crypto?

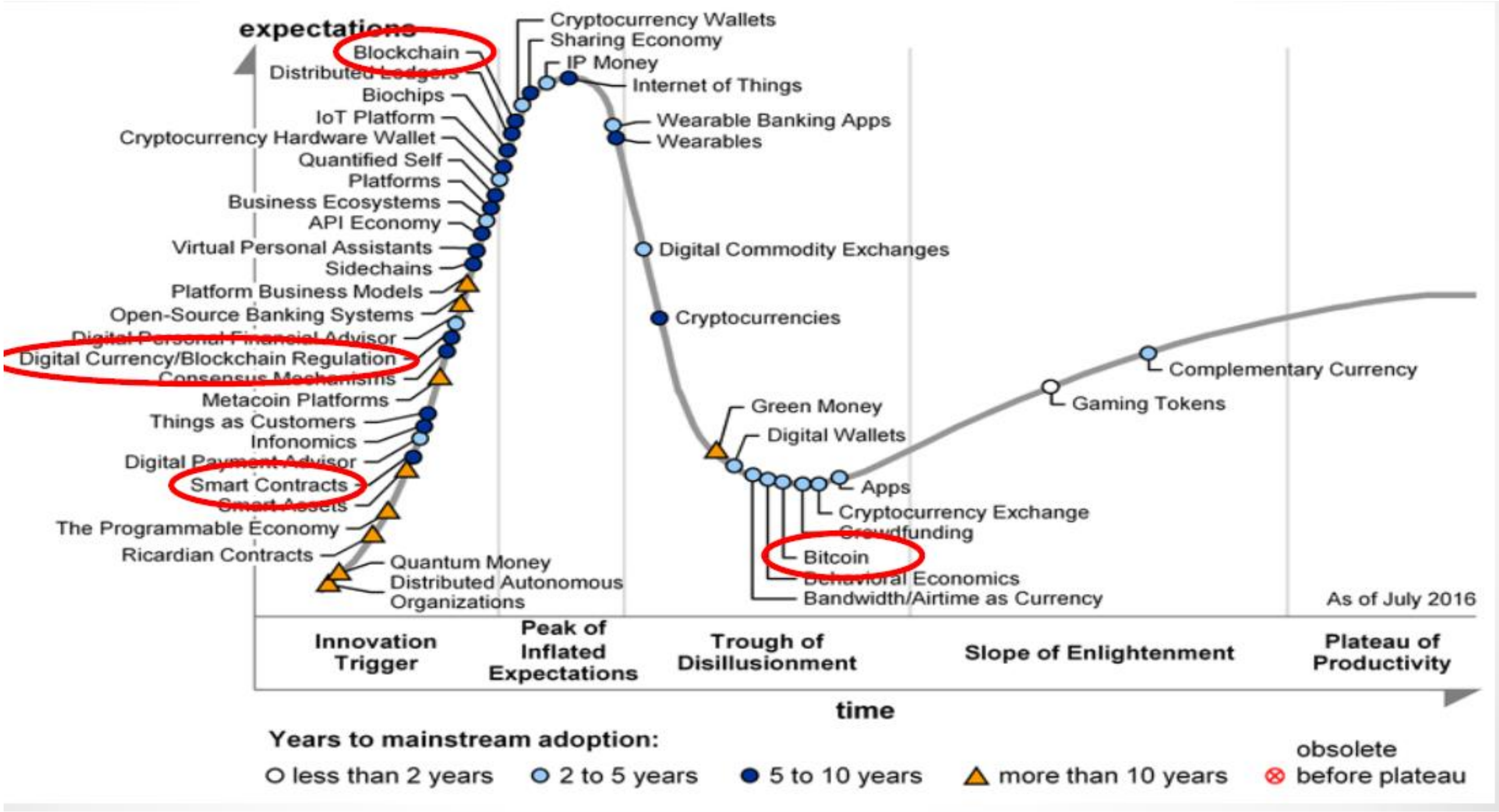
"File:08. Humpty Dumpty - panoramio.jpg" by Christopher Wood is licensed under CC BY-SA 3.0 (cropped)



# A blockchain is a chain of blocks



# Gartner hype cycle July 2016



# Gartner hype cycle July 2017

Where's Bitcoin?

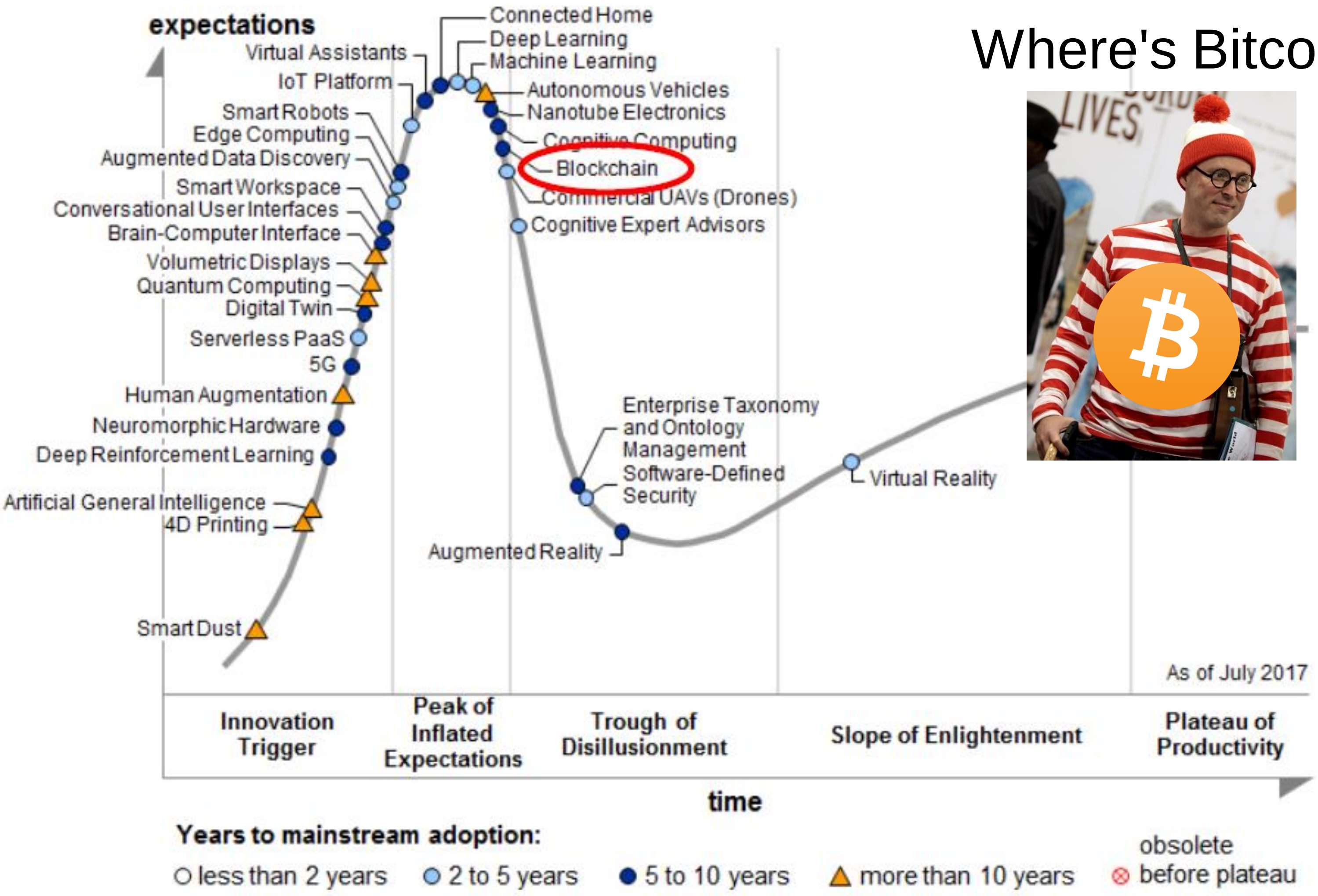
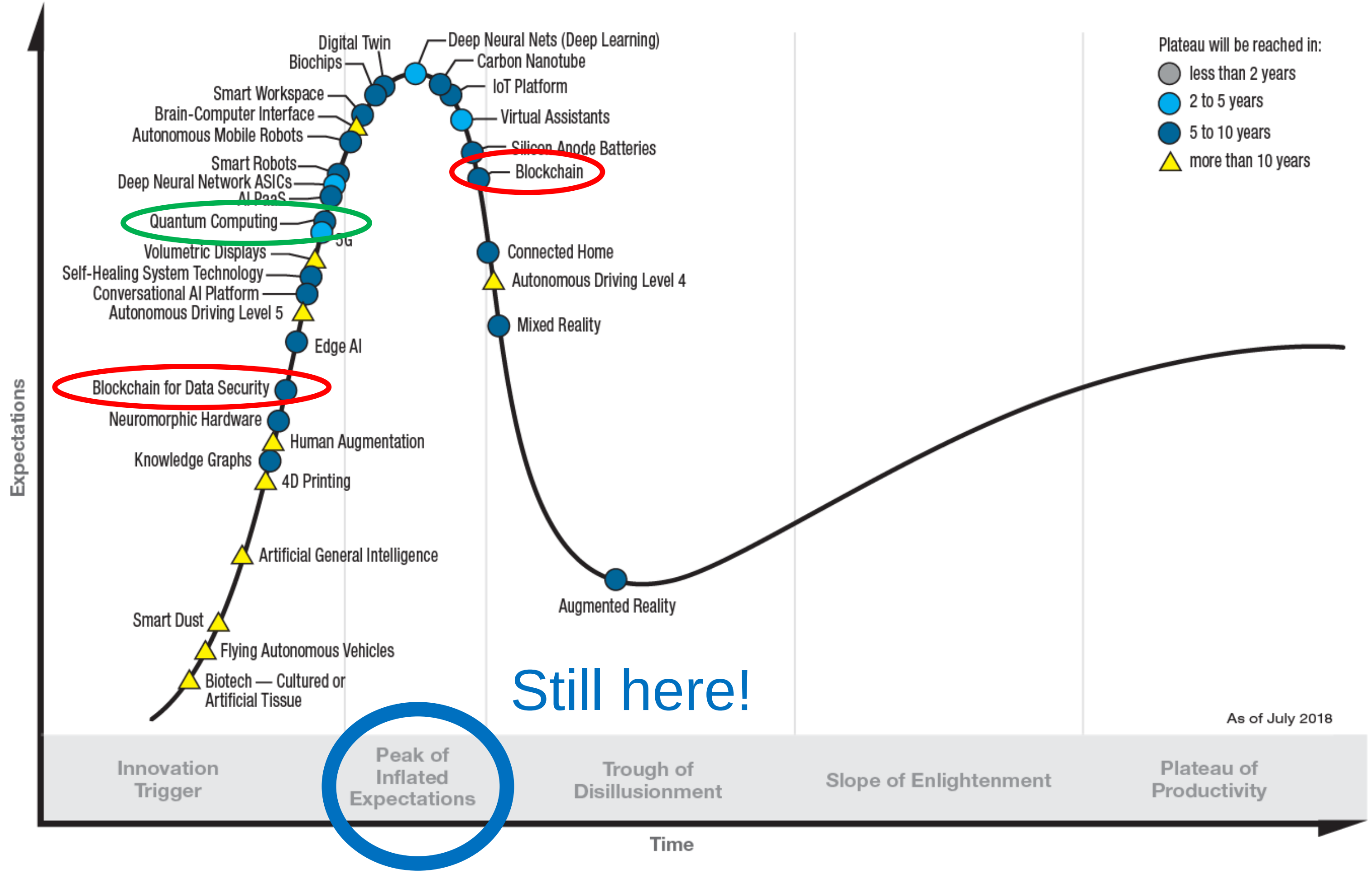


Photo by Gage Skidmore CC BY-SA 2-0

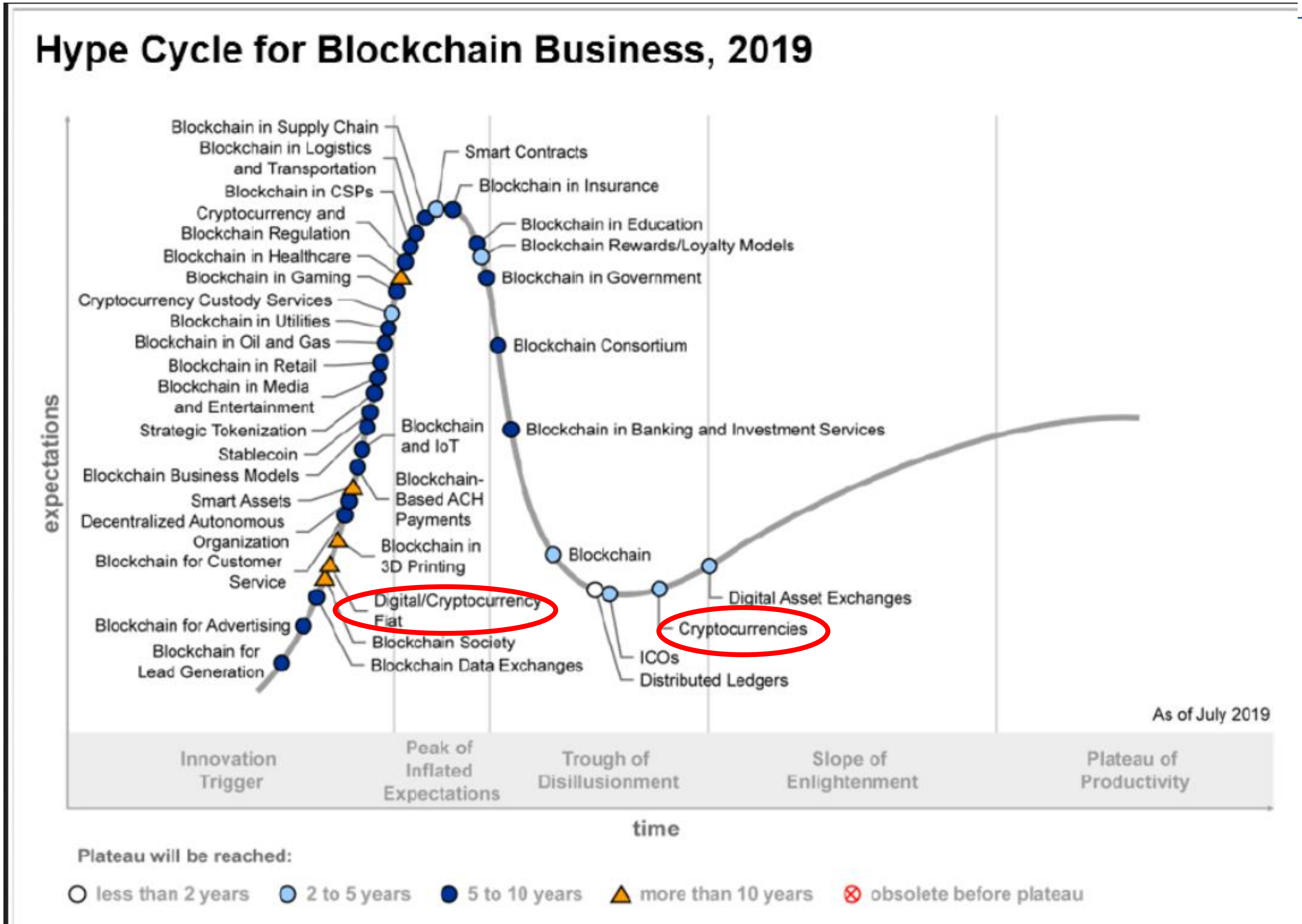
# Gartner hype cycle July 2018



Still here!

https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

# Still confused? Not after THIS episode


Hype Cycle for Blockchain Business, 2019

Source: Gartner
ID: 390391

https://emtemp.gcom.cloud/ngw/globalassets/en/newsroom/images/graphs/Blockchain-HC-2019.png

# What will quantum computing do?

- All digital signatures commonly in use today will be broken
- All hash algorithms will need to double their hash sizes (re: birthday paradox)

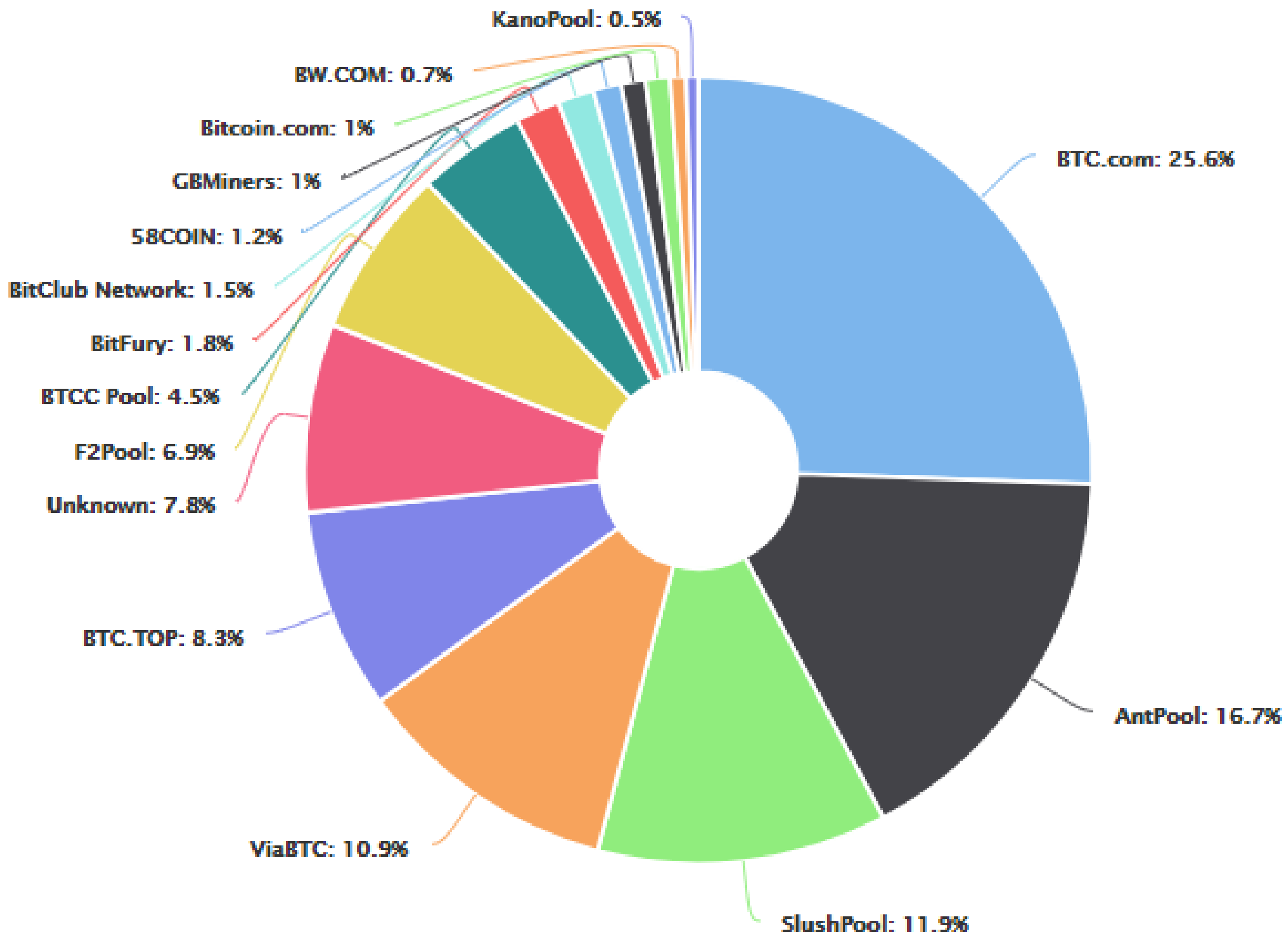
https://arxiv.org/abs/1804.00200

# Consensus on consensus algorithms?

- Proof of work
  - How much power do they use in Ireland, anyway?
- Proof of stake
  - The rich get richer?
- Round robin
  - Can the crooks make instances faster than you?
- Proof of elapsed time
- Byzantine Fault Tolerance

- There's a reason why distributed consensus has been a hard problem for half a century!

# Speaking of Bitcoin



Bitcoin Mining Pools

https://coinscage.com/best-bitcoin-mining-pools/

# Bitcoin price fluctuations last 6 months

$10 000

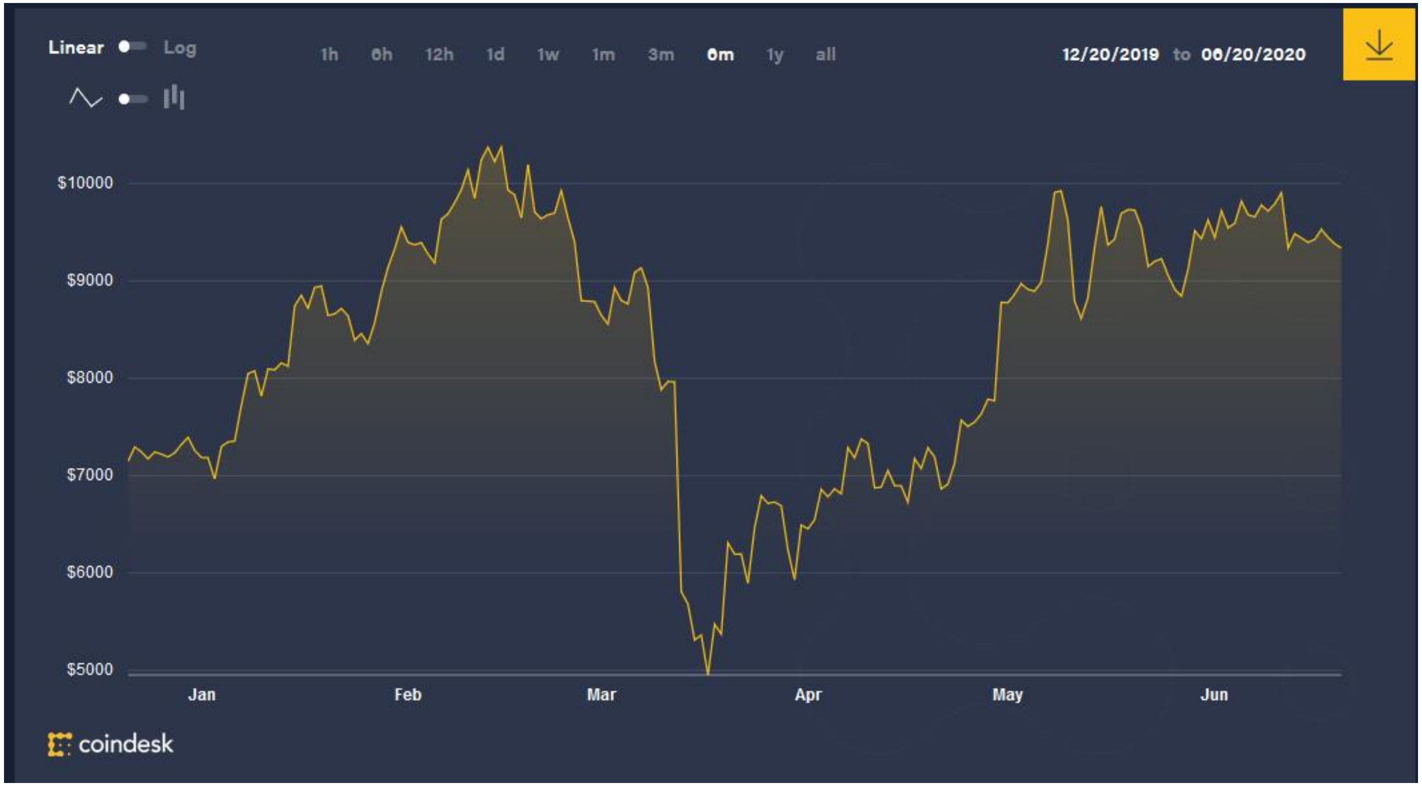
$ 9000

$8000

$7000

$6000

$5000



https://www.coindesk.com/price/bitcoin

# Blockchain Strengths & Opportunities

## Strengths

- Trust among untrusted Parties
- Distributed resilience and control
- Fully Decentralized network
- Primarily Open source
- Security and modern cryptography
- Controlled & Open Participation
- Dynamic and Fluid Operation

## Potential

- Reduced transaction costs
- Process acceleration & efficiency
- Reduced systemic risk
- Scalability & Timed Transactions
- Smart Contracts
- Bi-directional communication fabric
- New business-model enablement

Source: Gartner (March 2017)

# Not worried about censorship?

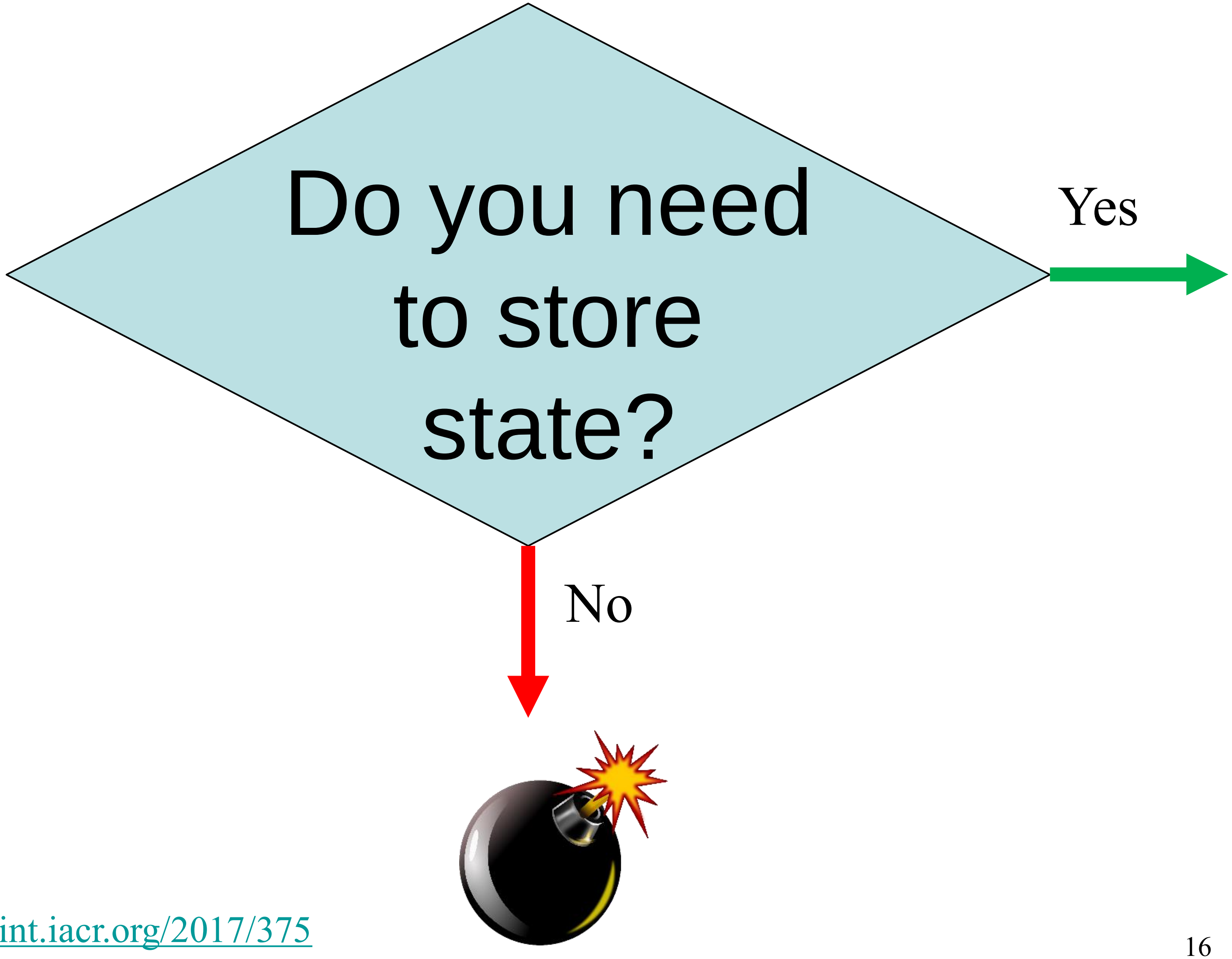
- Once information is on the blockchain, no government can remove it

# Do you need a blockchain?

Illustartion by Brianna Lehman; CC BY 2.0 https://www.flickr.com/photos/briannalehman/4252464937/

- Wüst and Gervais helpfully provided a flow chart

# State



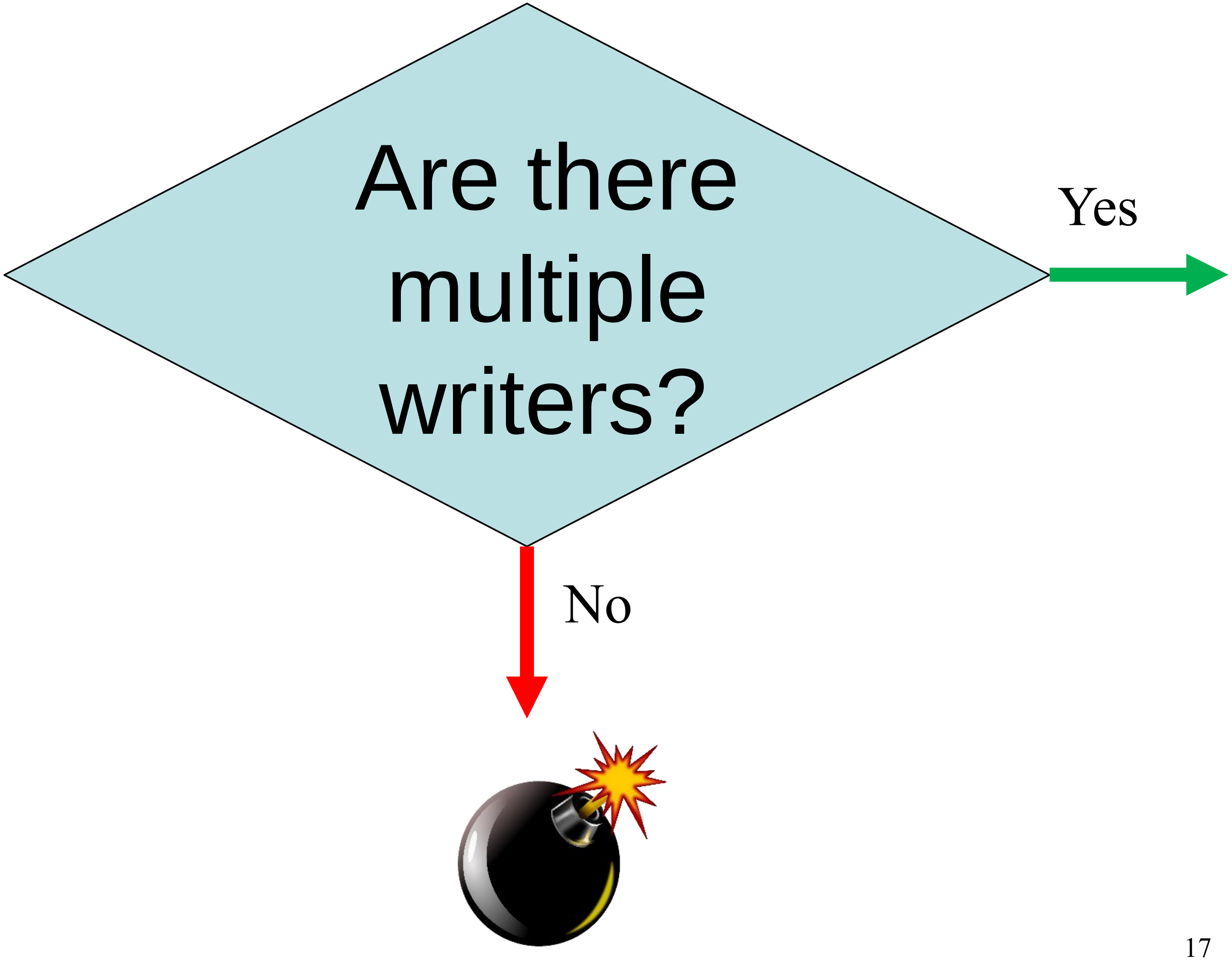
Do you need to store state?

Yes

No

https://eprint.iacr.org/2017/375

# Multiple writers

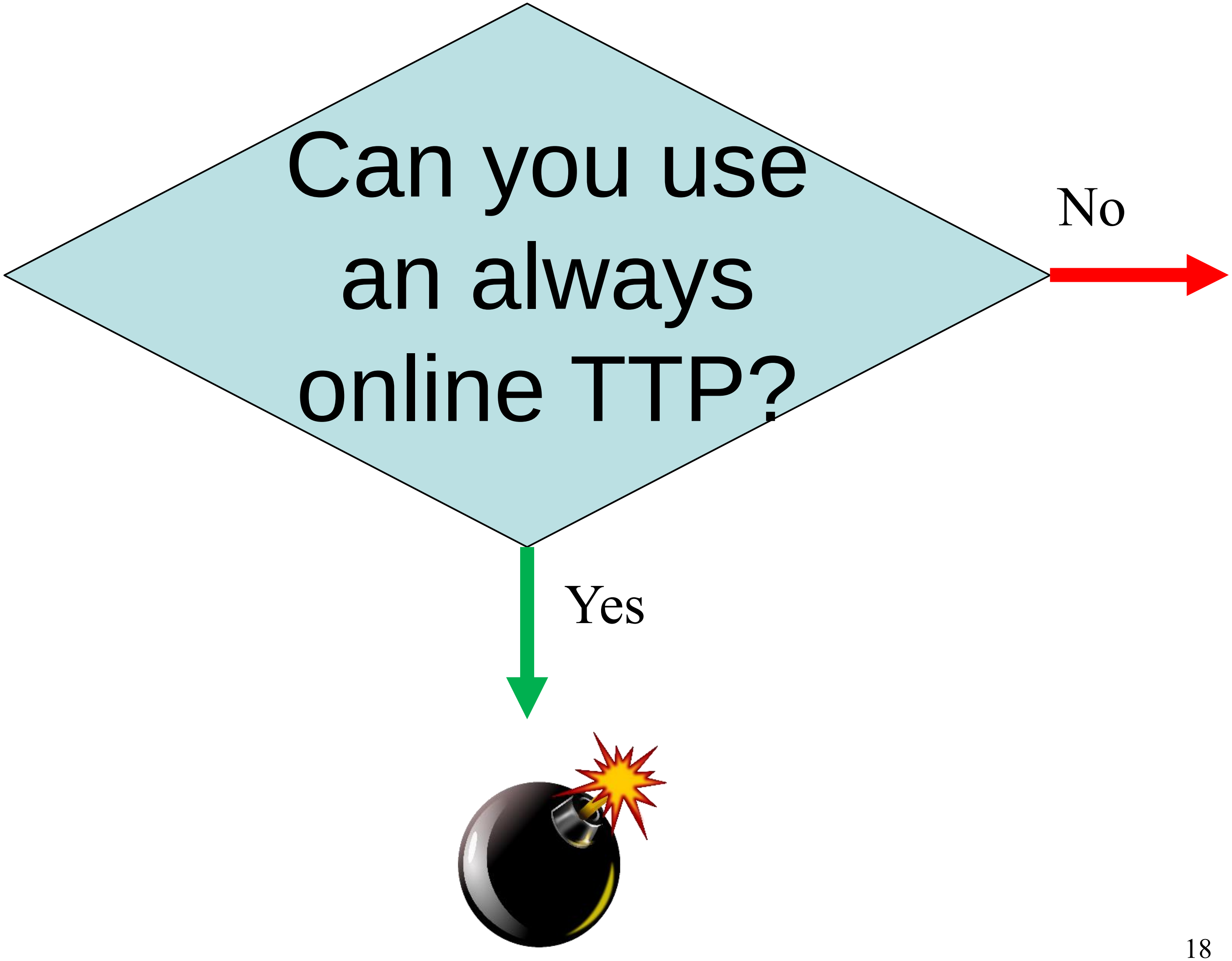


Are there multiple writers?

Yes

No

# TTP

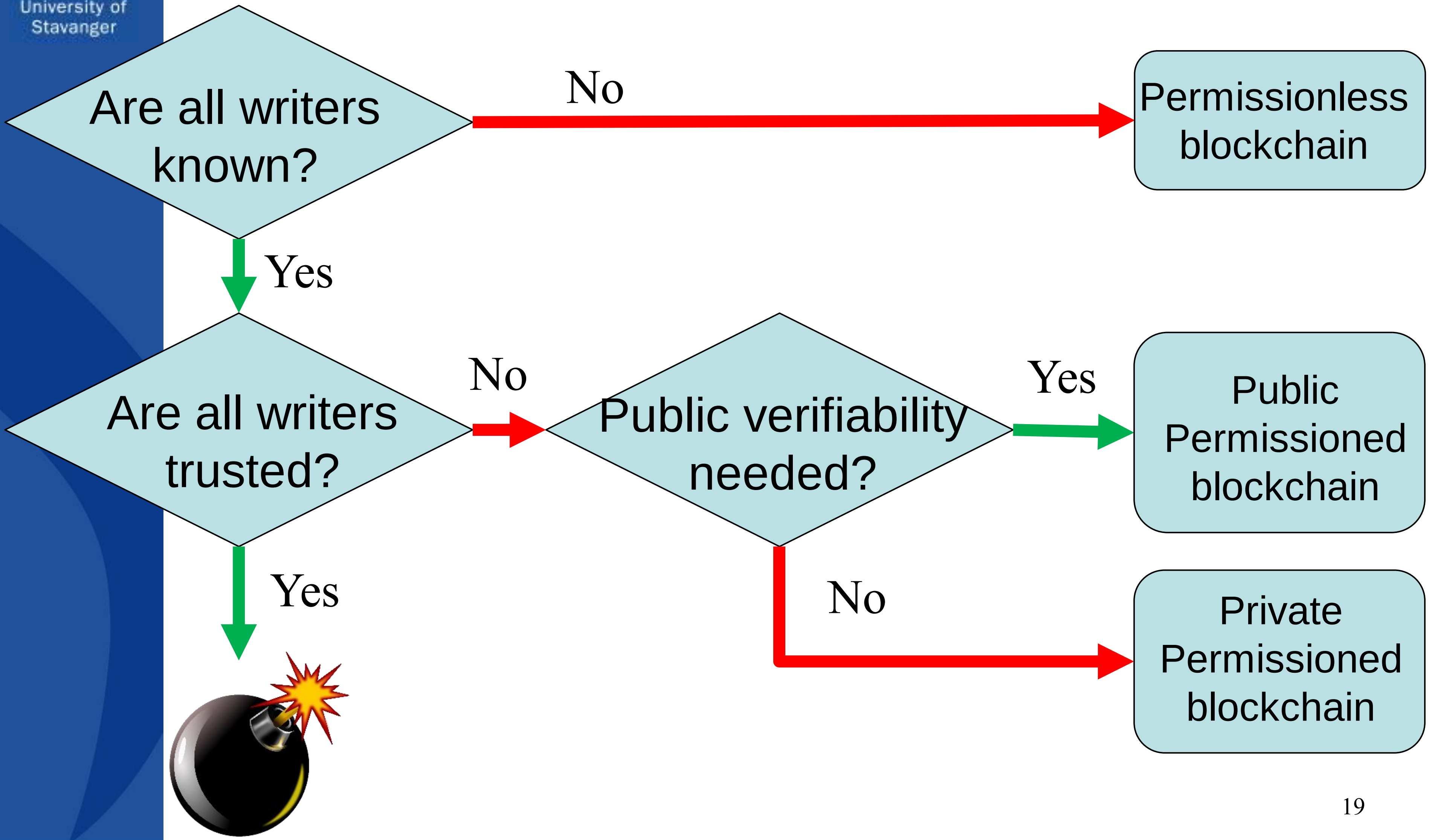


Can you use an always online TTP?

No

Yes

# Known and trusted



Are all writers known?

No

Permissionless blockchain

Yes

Are all writers trusted?

No

Public verifiability needed?

Yes

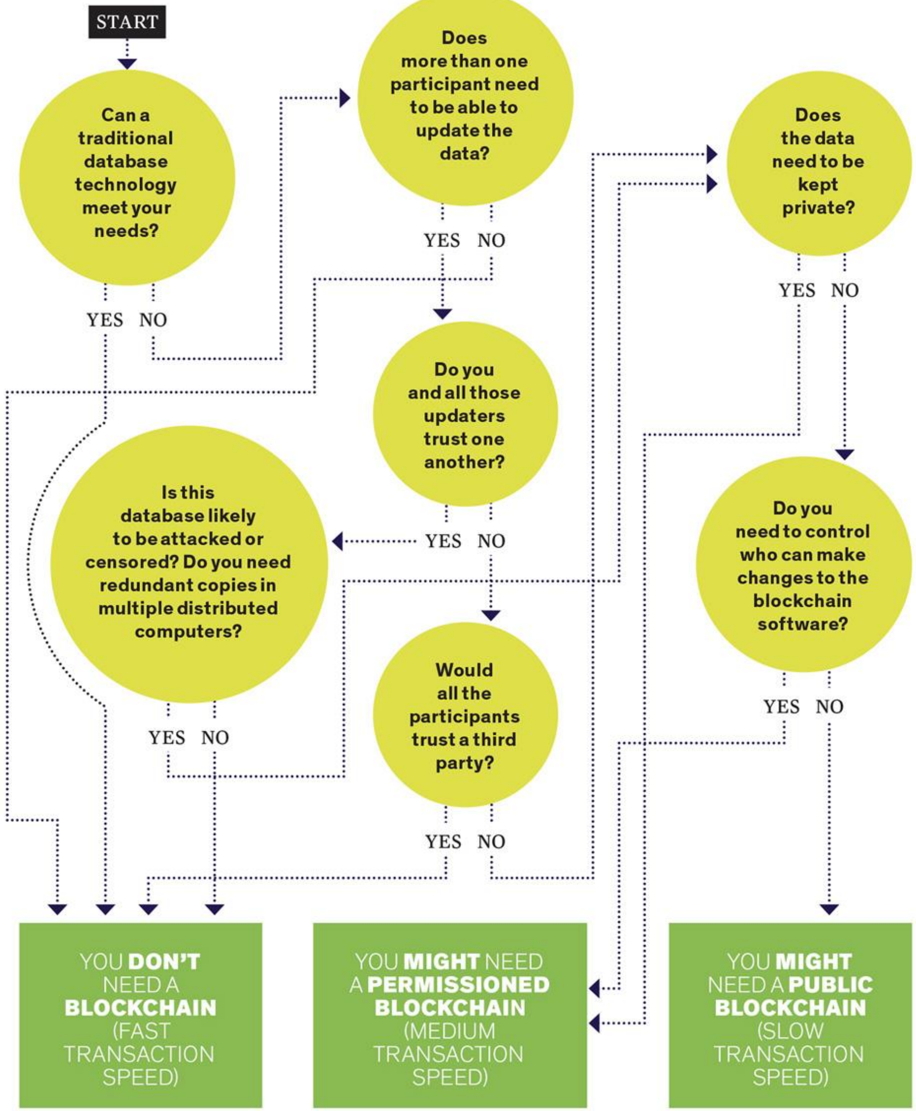
Public Permissioned blockchain

Yes

No

Private Permissioned blockchain

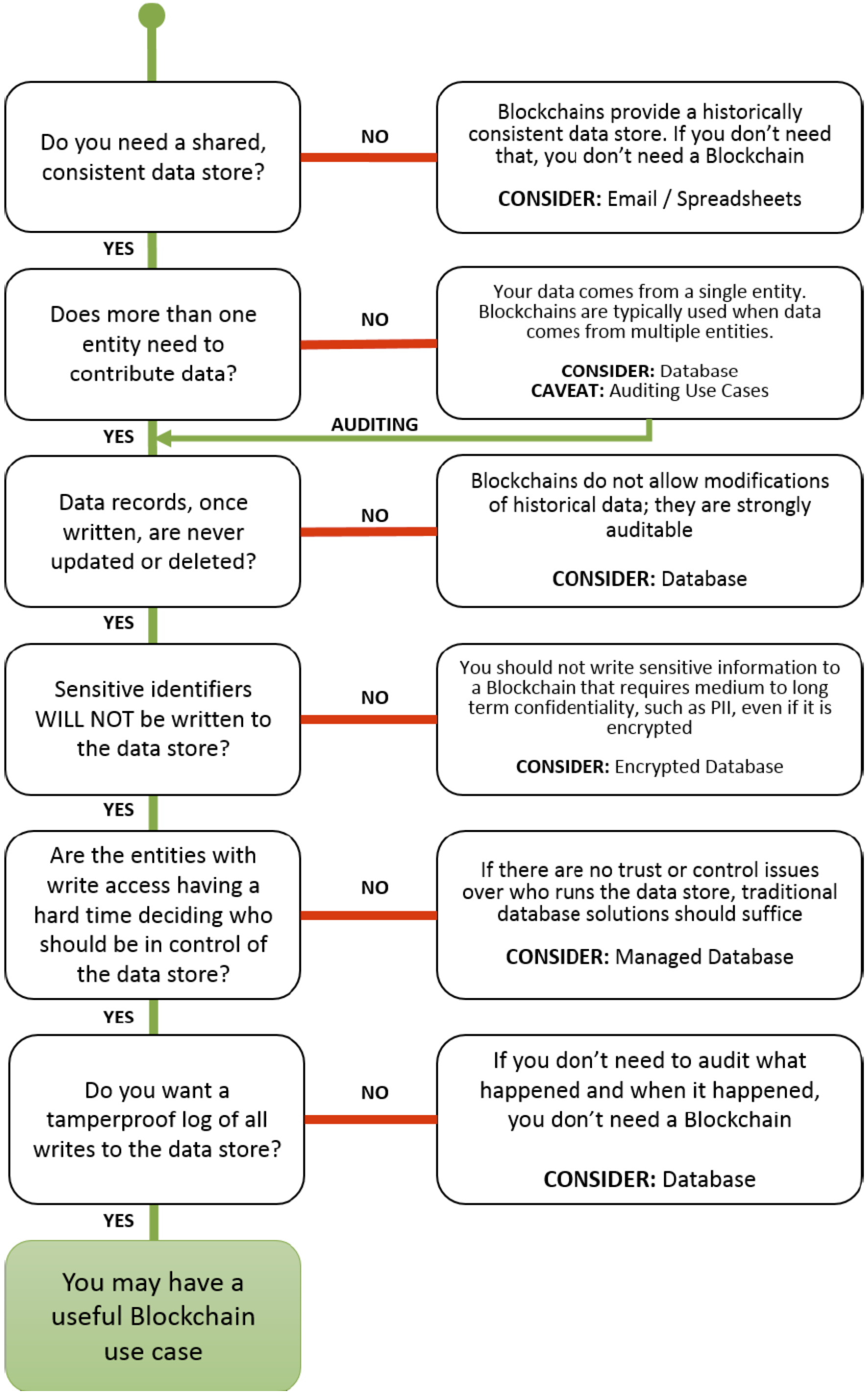
# Or, according to IEEE Spectrum


START
Can a traditional database technology meet your needs?
YES
NO
Does more than one participant need to be able to update the data?
YES
NO
Do you and all those updaters trust one another?
YES
NO
Is this database likely to be attacked or censored? Do you need redundant copies in multiple distributed computers?
YES
NO
Would all the participants trust a third party?
YES
NO
Does the data need to be kept private?
YES
NO
Do you need to control who can make changes to the blockchain software?
YES
NO
YOU DON'T NEED A BLOCKCHAIN (FAST TRANSACTION SPEED)
YOU MIGHT NEED A PERMISSIONED BLOCKCHAIN (MEDIUM TRANSACTION SPEED)
YOU MIGHT NEED A PUBLIC BLOCKCHAIN (SLOW TRANSACTION SPEED)

https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain

# Or NIST…

https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf



Do you need a shared, consistent data store?

NO

Blockchains provide a historically consistent data store. If you don't need that, you don't need a Blockchain

**CONSIDER:** Email / Spreadsheets

YES

Does more than one entity need to contribute data?

NO

Your data comes from a single entity. Blockchains are typically used when data comes from multiple entities.

**CONSIDER:** Database
**CAVEAT:** Auditing Use Cases

AUDITING

YES

Data records, once written, are never updated or deleted?

NO

Blockchains do not allow modifications of historical data; they are strongly auditable

**CONSIDER:** Database

YES

Sensitive identifiers WILL NOT be written to the data store?

NO

You should not write sensitive information to a Blockchain that requires medium to long term confidentiality, such as PII, even if it is encrypted

**CONSIDER:** Encrypted Database

YES

Are the entities with write access having a hard time deciding who should be in control of the data store?

NO

If there are no trust or control issues over who runs the data store, traditional database solutions should suffice

**CONSIDER:** Managed Database

YES

Do you want a tamperproof log of all writes to the data store?

NO

If you don't need to audit what happened and when it happened, you don't need a Blockchain

**CONSIDER:** Database

YES

You may have a useful Blockchain use case

# Remember:
# Blockchain is not your only tool!

- Now, on to the five things…

# 1. Online voting

- Still need to trust the central authority!
- Creating ballots, authenticating voters…
- Other security concerns also remain

# 2. Supply chain management

- If all parties can be trusted to contribute to the final product, why not to write supply chain data?
- Interface between physical and digital world
- Detecting counterfeit drugs – why not use a digital signature?

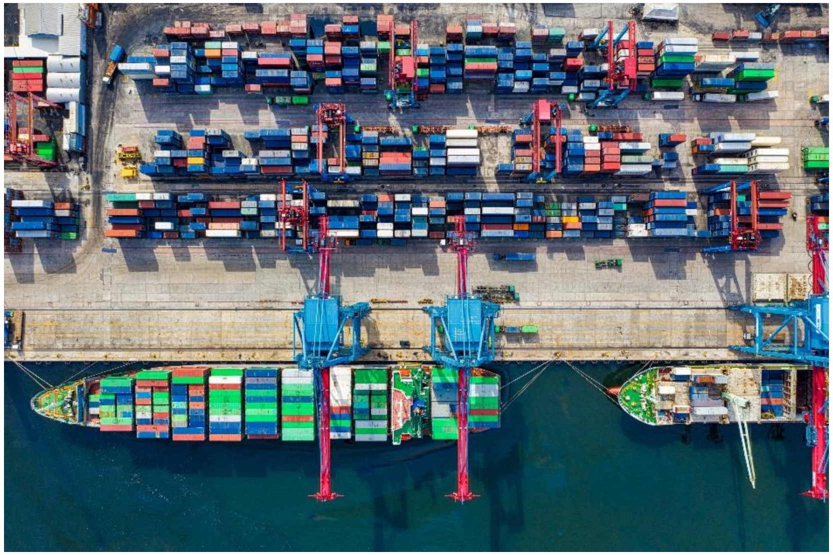


Photo by Tom Fisk from Pexels

# 3. Internet of things with no internet

- Interface between physical and digital world (again)
- If you compromise the "thing", all bets are off.

# 4. Distributed network for calculations

- An enormous redundancy of computing power
- No real parallelism
- No coordinated operations
- No efficiency

Photo by panumas nikhomkhai from Pexels

# 5. Storage of confidential data (1)

- GDPR!
- Right to be forgotten
- Once said, it cannot be unsaid

# But can't we just encrypt everything?

Illustration by Simon James https://www.flickr.com/photos/bearpark/2817161488/ CC BY 2.0

# 5. Storage of confidential data (2)

- An encrypted string can decrypt to anything, depending on the key:

```
The answer to life, the universe and everything is 42
```

or

```
Donald is a really nice guy who just wants 2 have fun
```

- It doesn't help if the blockchain is tamper resistant, if I can just change the key!

# A final question…

# Thank you for your attention!

- http://www.sislab.no/rbchain/
- https://stc.computer.org/blockchain/
- https://infosec.sintef.no/

IEEE CS STC
Blockchain

University of Stavanger