UNSW SYDNEY | Australia's Global University

Blockchain for Cyberphysical Systems

~~Keynote~~ conversation starter

Salil Kanhere

School of Computer Science and Engineering

UNSW Sydney

Australia

E: salil.kanhere@unsw.edu.au

W: www.salilkanhere.net

Acknowledgements

UNSW: Ali Dorri, Sidra Malik, Chuka Oham, Pooja Gupta, Sanjay Jha, Joe Dong

Data61 CSIRO: Raja Jurdak

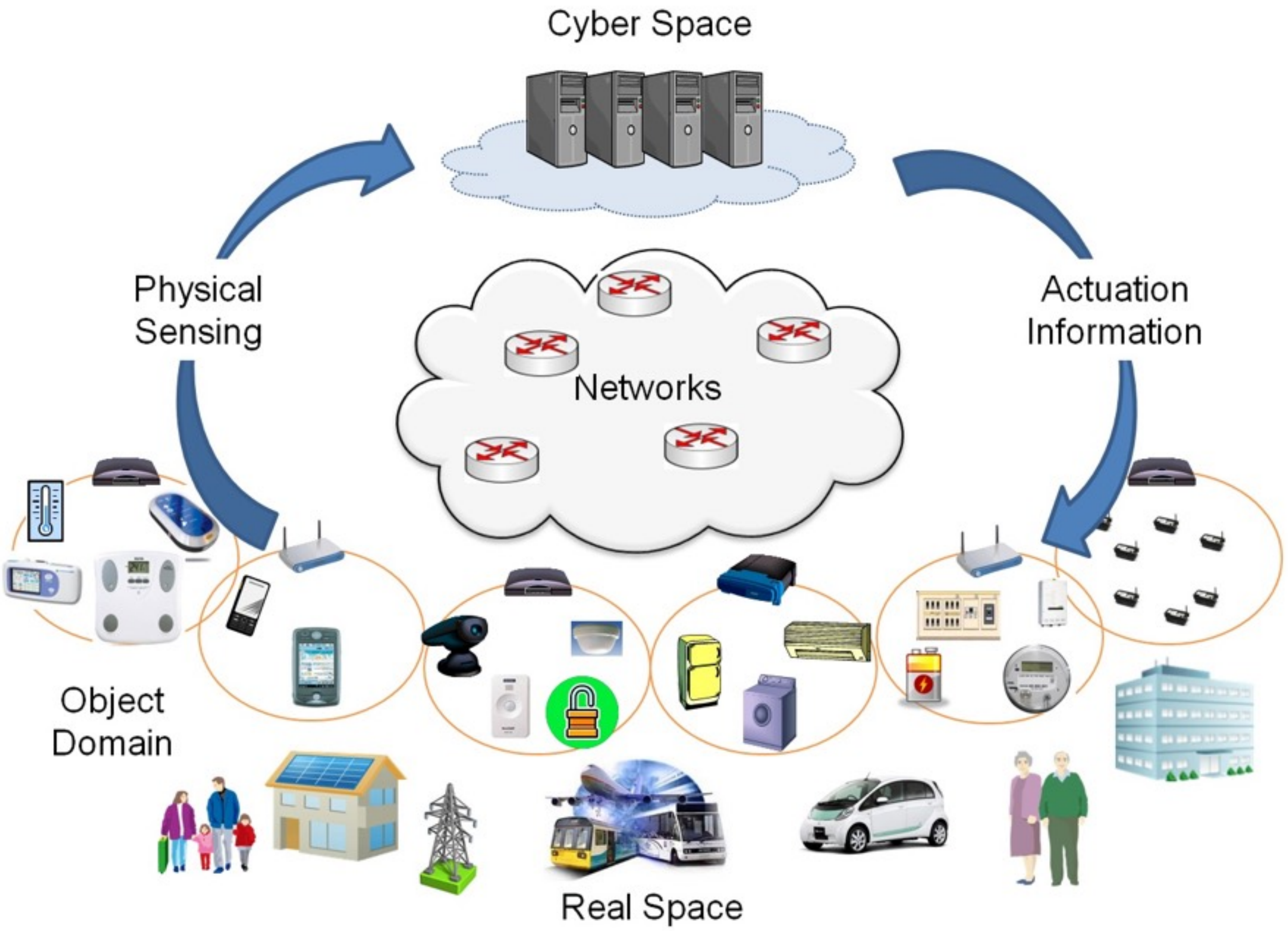
TCS Australia: Praveen Gauravaram

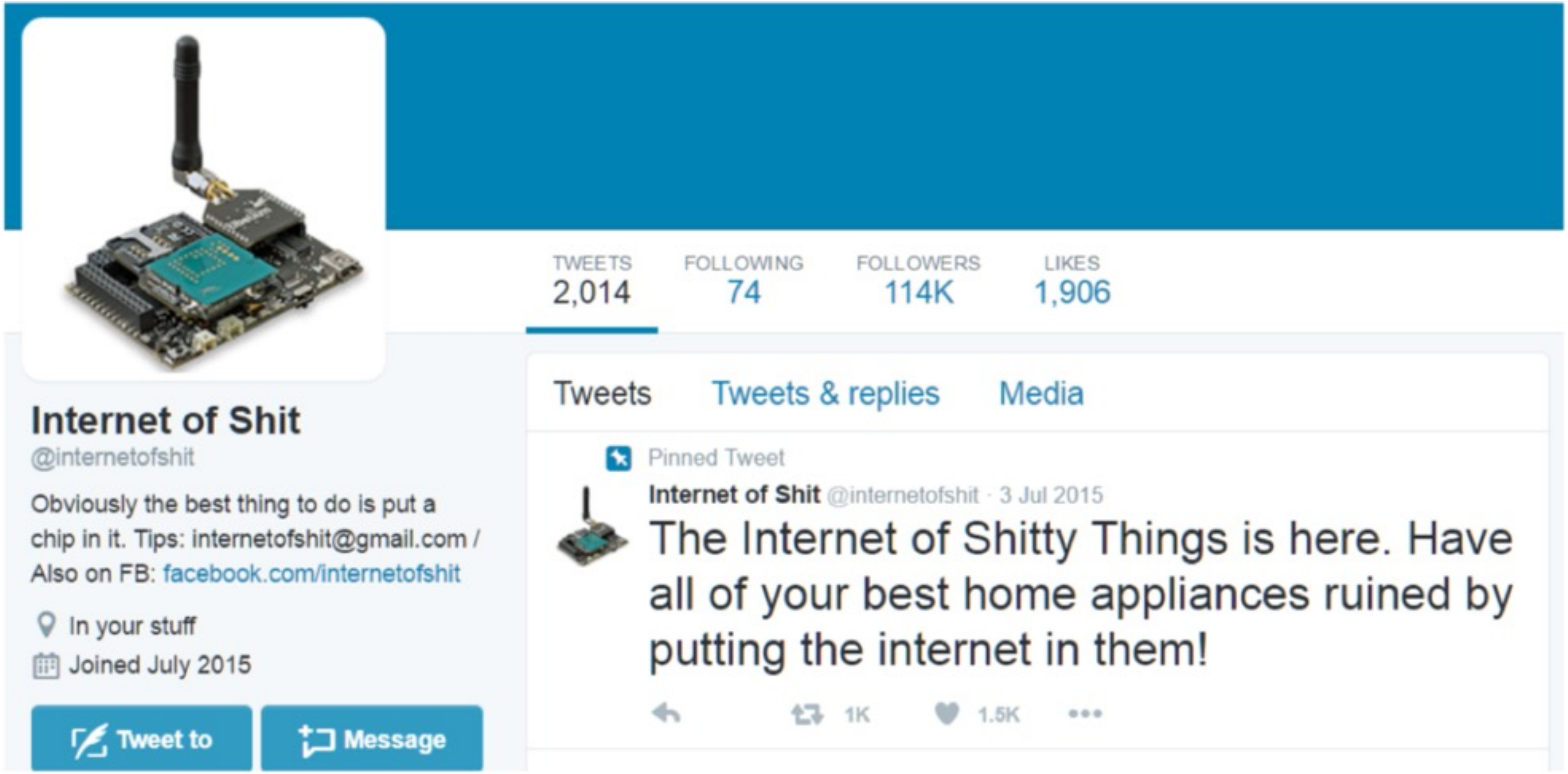
Virtual Vehicle Center/TU Graz: Marco Steger

Pontifical Universidade Catolica do Rio Grande do Sul: Regio Michelin, Roben Castagna Lunardi, Avelino Francisco Zorzo

I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
S. Adams E-mail: SCOTTADAMS@AOL.COM
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
© 1995 United Feature Syndicate, Inc.(NYC)
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.

Cyberphysical = tight conjoining of and coordination between computation and physical resources





TWEETS 2,014 FOLLOWING 74 FOLLOWERS 114K LIKES 1,906

Internet of Shit

@internetofshit

Obviously the best thing to do is put a chip in it. Tips: internetofshit@gmail.com / Also on FB: facebook.com/internetofshit

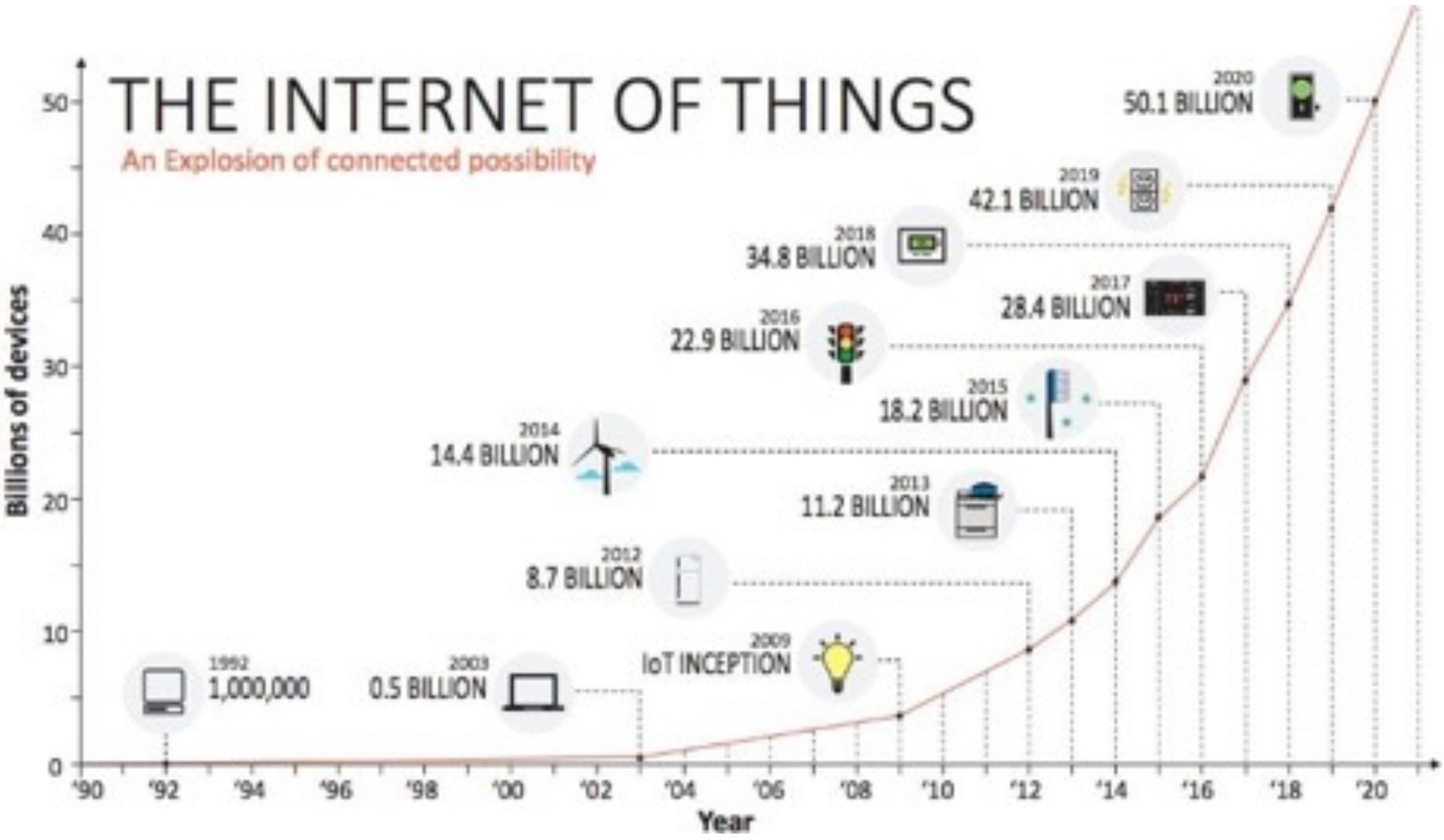
In your stuff

Joined July 2015

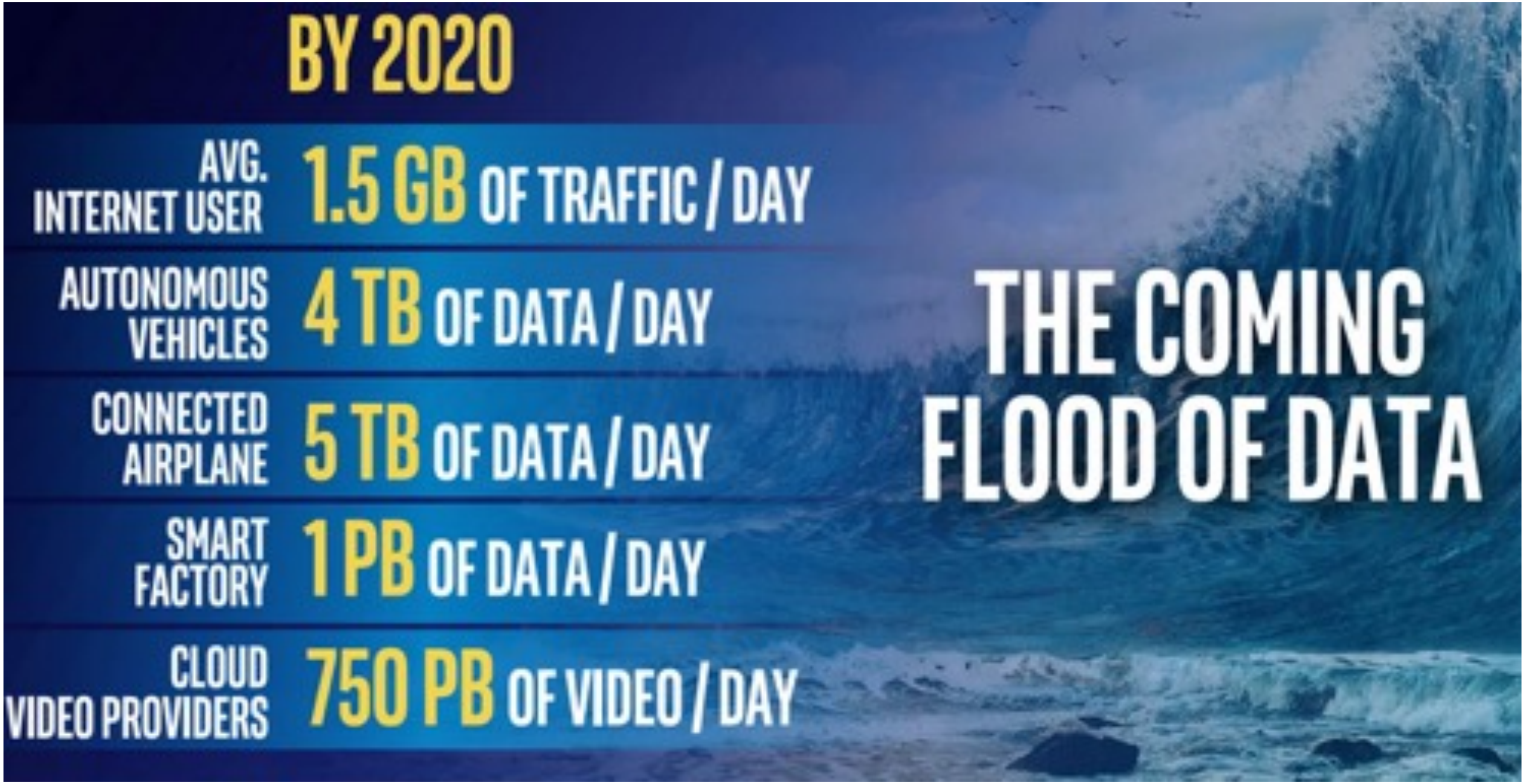
Pinned Tweet

Internet of Shit @internetofshit · 3 Jul 2015

The Internet of Shitty Things is here. Have all of your best home appliances ruined by putting the internet in them!



Source: Intel



BY 2020

AVG. INTERNET USER	1.5 GB	OF TRAFFIC / DAY
AUTONOMOUS VEHICLES	4 TB	OF DATA / DAY
CONNECTED AIRPLANE	5 TB	OF DATA / DAY
SMART FACTORY	1 PB	OF DATA / DAY
CLOUD VIDEO PROVIDERS	750 PB	OF VIDEO / DAY

THE COMING FLOOD OF DATA

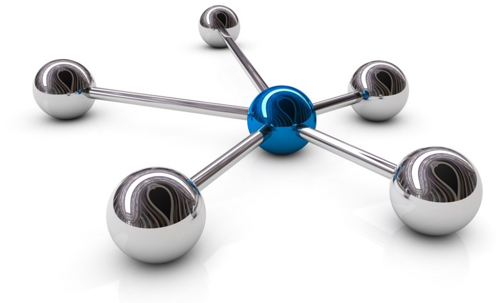
Source: Intel

Current IoT Ecosystems

3 Tiers:

- Low-power IoT devices
- Gateway
- Cloud

Centralization does not scale



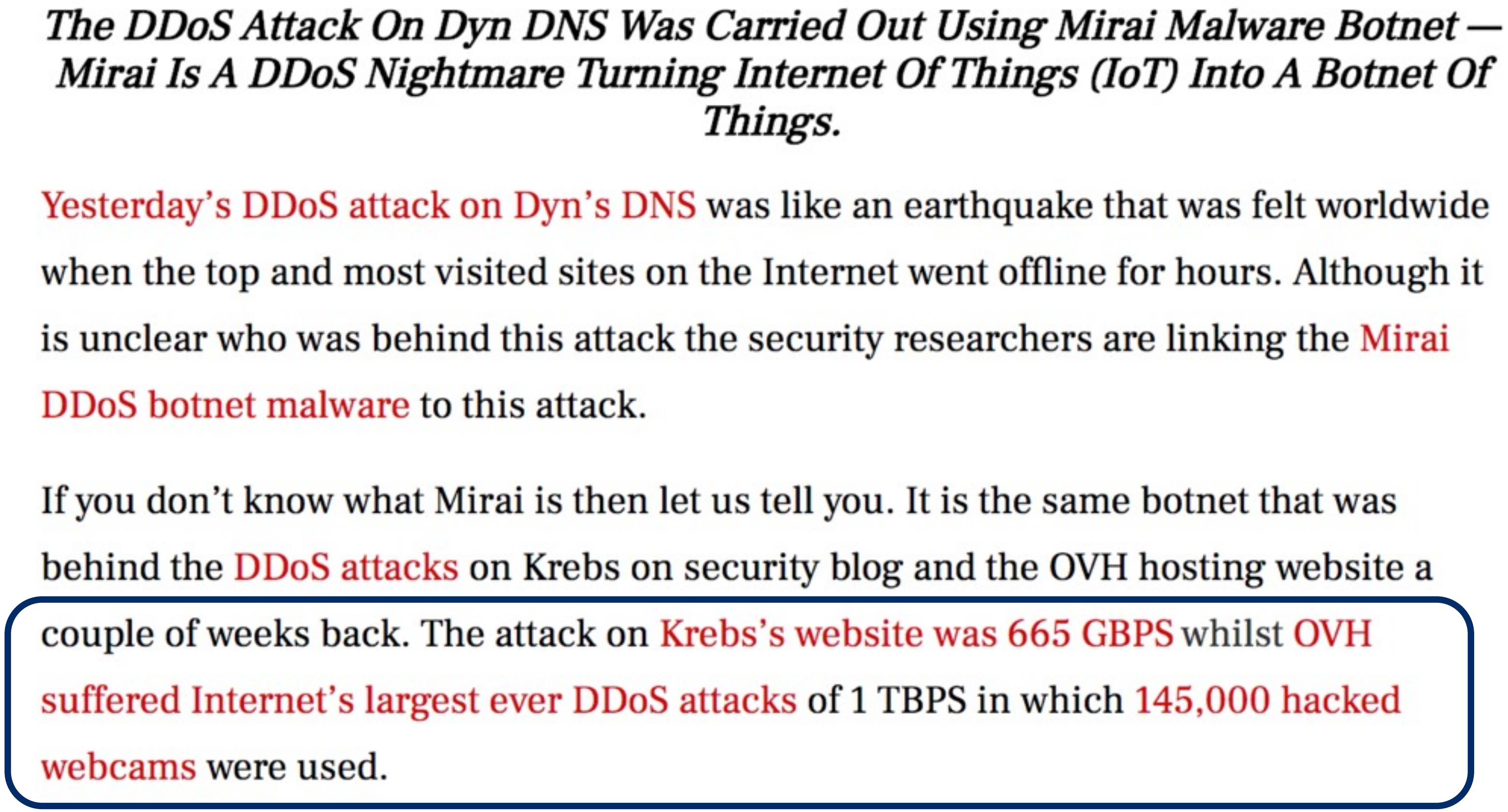
Centralised brokered communication models based on the client-server paradigm

All devices are identified, authenticated and connected through cloud servers

Often, two IoT devices sitting next to each other will communicate through the Internet

Security and privacy is a significant challenge

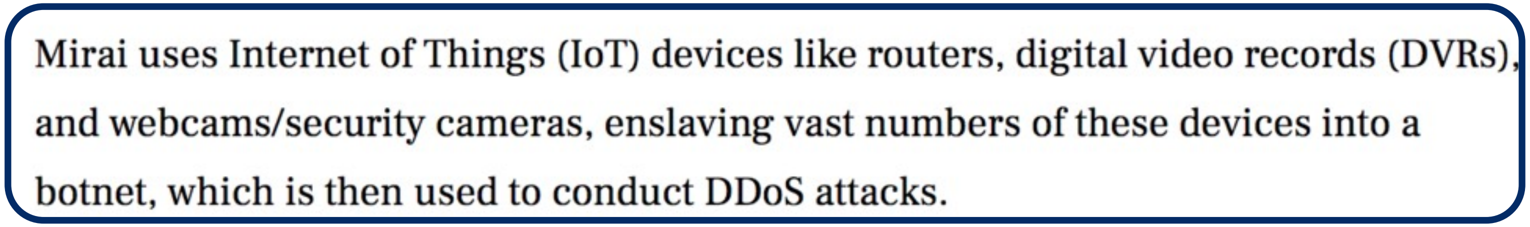
Source: Hackread



The DDoS Attack On Dyn DNS Was Carried Out Using Mirai Malware Botnet — Mirai Is A DDoS Nightmare Turning Internet Of Things (IoT) Into A Botnet Of Things.

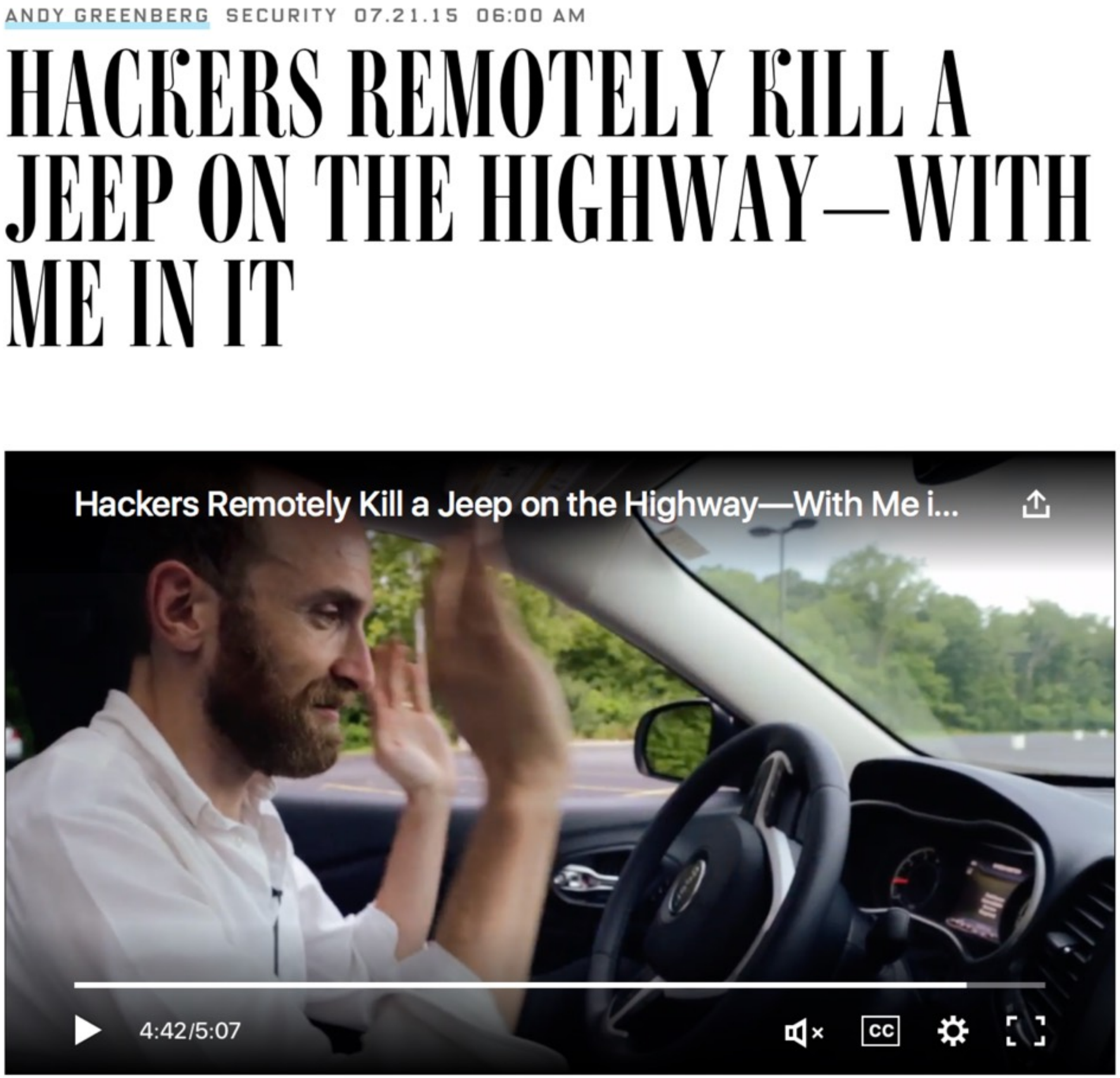
Yesterday's DDoS attack on Dyn's DNS was like an earthquake that was felt worldwide when the top and most visited sites on the Internet went offline for hours. Although it is unclear who was behind this attack the security researchers are linking the Mirai DDoS botnet malware to this attack.

If you don't know what Mirai is then let us tell you. It is the same botnet that was behind the DDoS attacks on Krebs on security blog and the OVH hosting website a couple of weeks back. The attack on Krebs's website was 665 GBPS whilst OVH suffered Internet's largest ever DDoS attacks of 1 TBPS in which 145,000 hacked webcams were used.



Mirai uses Internet of Things (IoT) devices like routers, digital video records (DVRs), and webcams/security cameras, enslaving vast numbers of these devices into a botnet, which is then used to conduct DDoS attacks.

Source: Hackread, Oct 2016



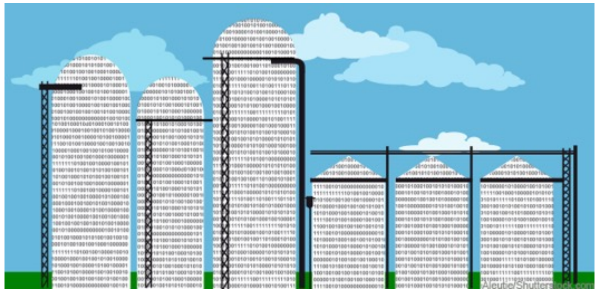
ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

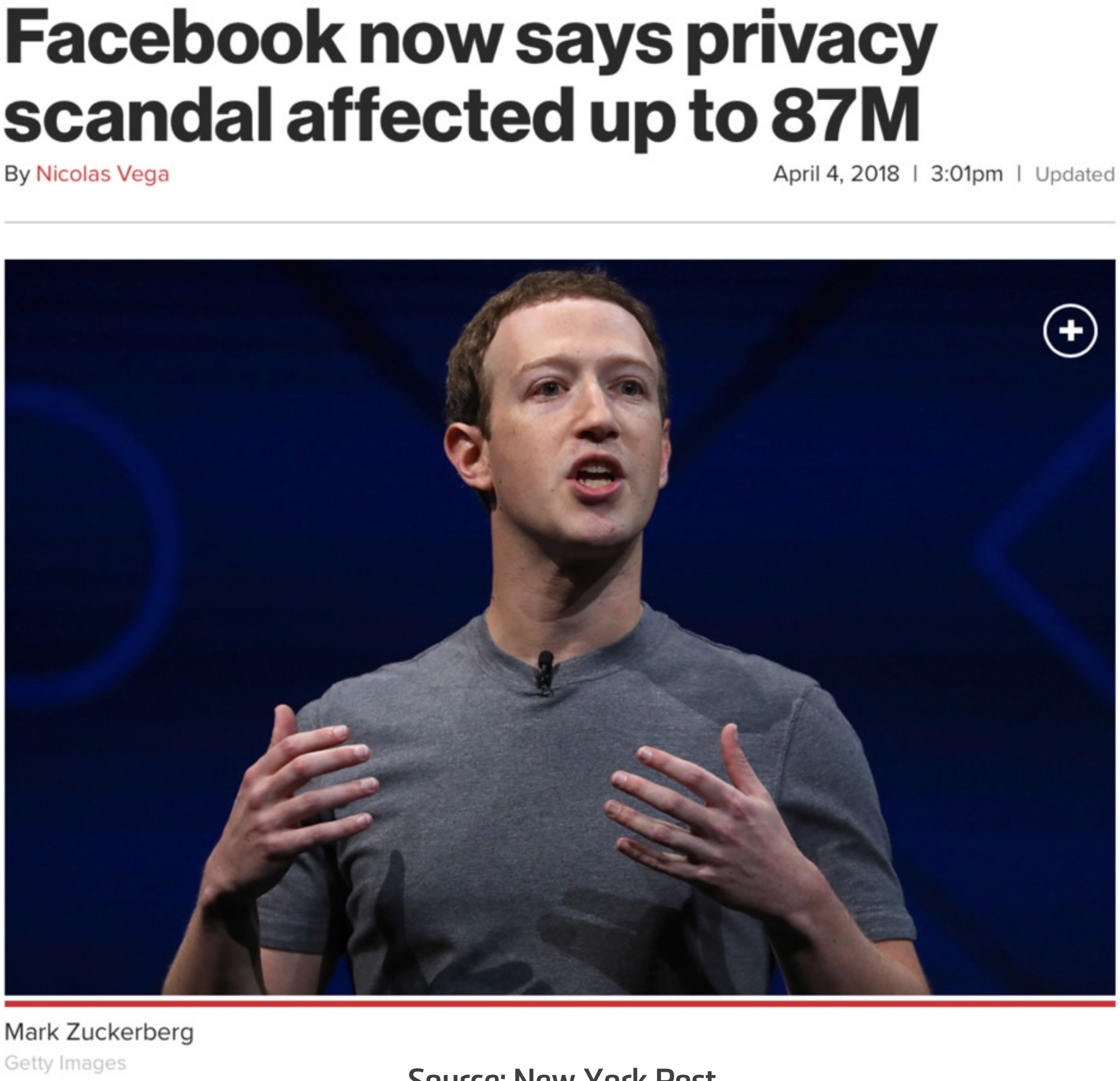
Hackers Remotely Kill a Jeep on the Highway—With Me i...

Source: Wired, July 2015

Data Silos



- Isolated data silos
- We have limited control over our data and how it is used
- We have to trust the cloud and application providers
- This problem will exacerbate as IoT devices collect highly personal data



Facebook now says privacy scandal affected up to 87M

By Nicolas Vega

April 4, 2018 | 3:01pm | Updated

Mark Zuckerberg

Getty Images

Source: New York Post

Challenges facing CPS

- Heterogeneity in device resources
- Multiple attack surfaces
- Scale
- Centralization
- Lack of control over how data is shared/used and lack of auditability
- Complex interactions of different OS/software stacks/hardware
- Poor implementation of security/privacy mechanisms
- ……..

IS THERE ANOTHER WAY FORWARD?
imgflip.com

BLOCKCHAIN IS THE ANSWER
imgflip.com

Inventor: Satoshi Nakomoto
https://bitcoin.org/bitcoin.pdf

How the Bitcoin Blockchain Works

1. Alice sends Bob some bitcoins in a digitally signed transaction

2. The transaction is broadcast to the entire network

3. Miners around the world race each other to solve a "Proof of Work" puzzle

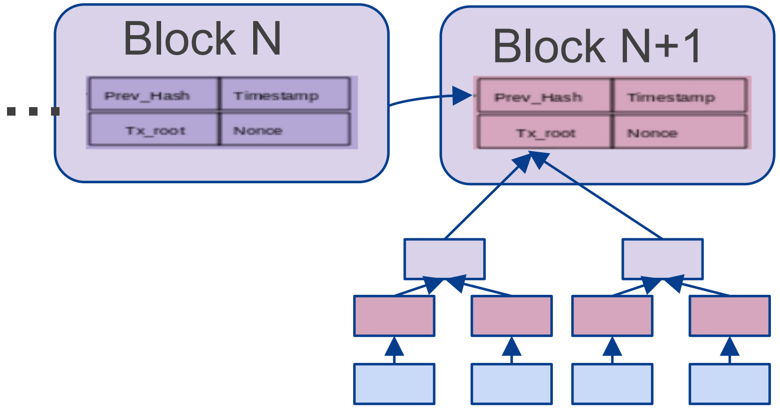
4. Winner combines pending transactions into a "block" & collects fees. This happens every ~10 minutes.

5. The new block is broadcast to the entire network and added to the "chain"

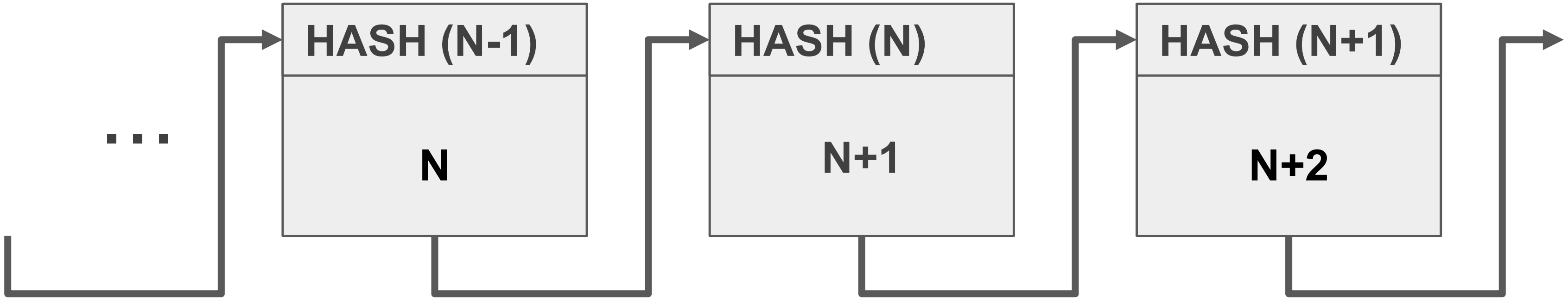
6. In case of conflicts, the longest chain wins; this results in consensus on which blocks are on the chain.

7. Any transaction that is 3-4 blocks into the blockchain cannot, for all practical purposes, be reversed.

8. Bob can use wallet software to verify the transaction doesn't involve Alice "double spending" her money



Blockchain Data Structure



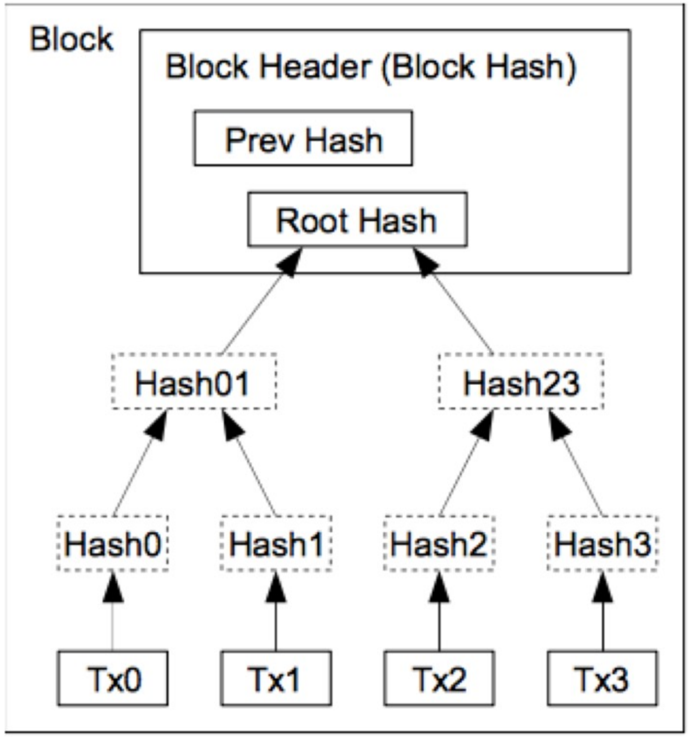
Each transaction is a digitally signed set of input and output addresses

Each block is a collection of transactions

Proof of Work: A miner must find a “nonce” such that the hash of a block contains a certain number of leading zeros

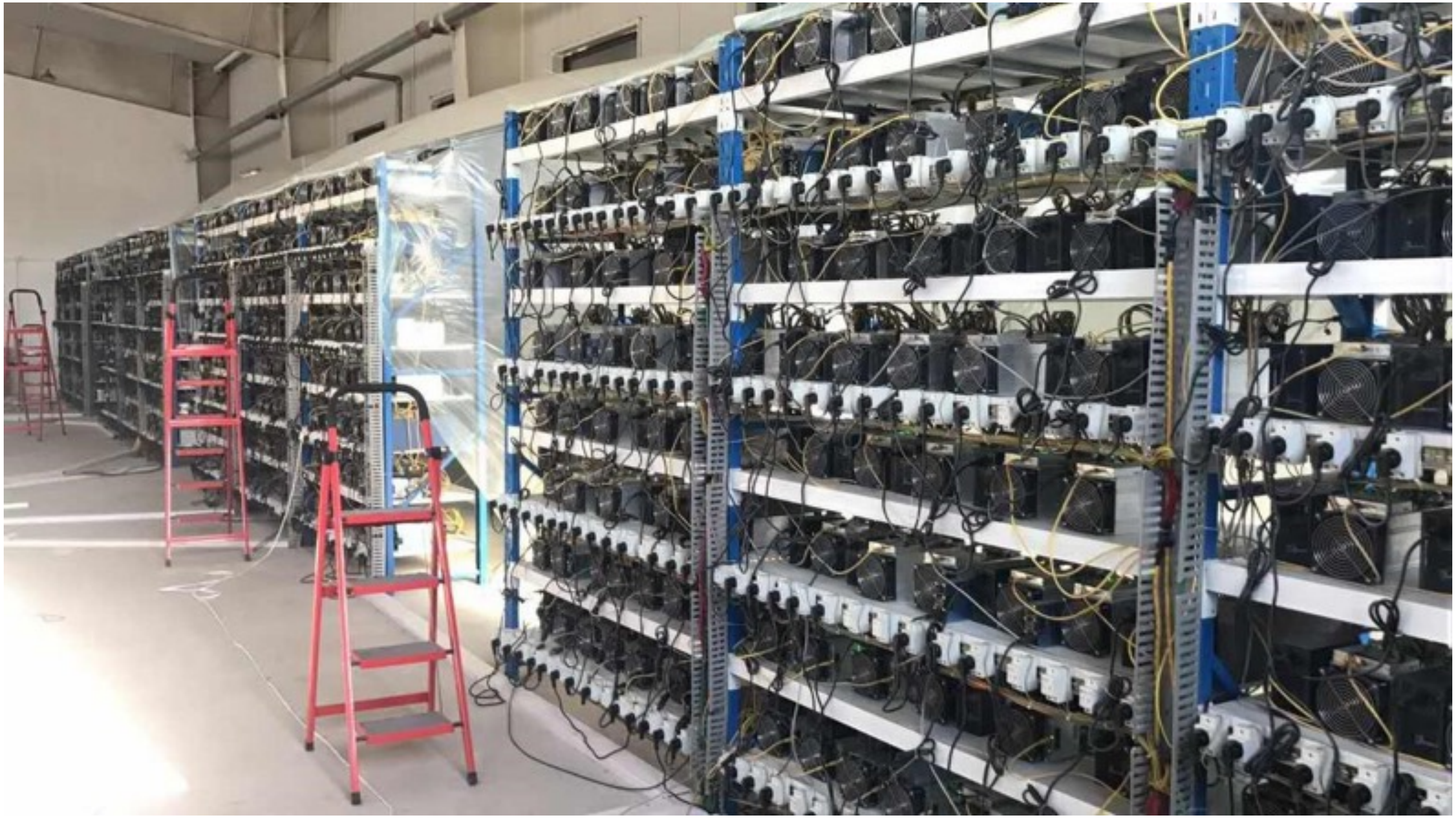
Within each block, the transactions are stored in the form of a Merkle tree which allows quick verification of (non) membership

Merkle Tree



Transactions Hashed in a Merkle Tree

A Bitcoin “Mine”



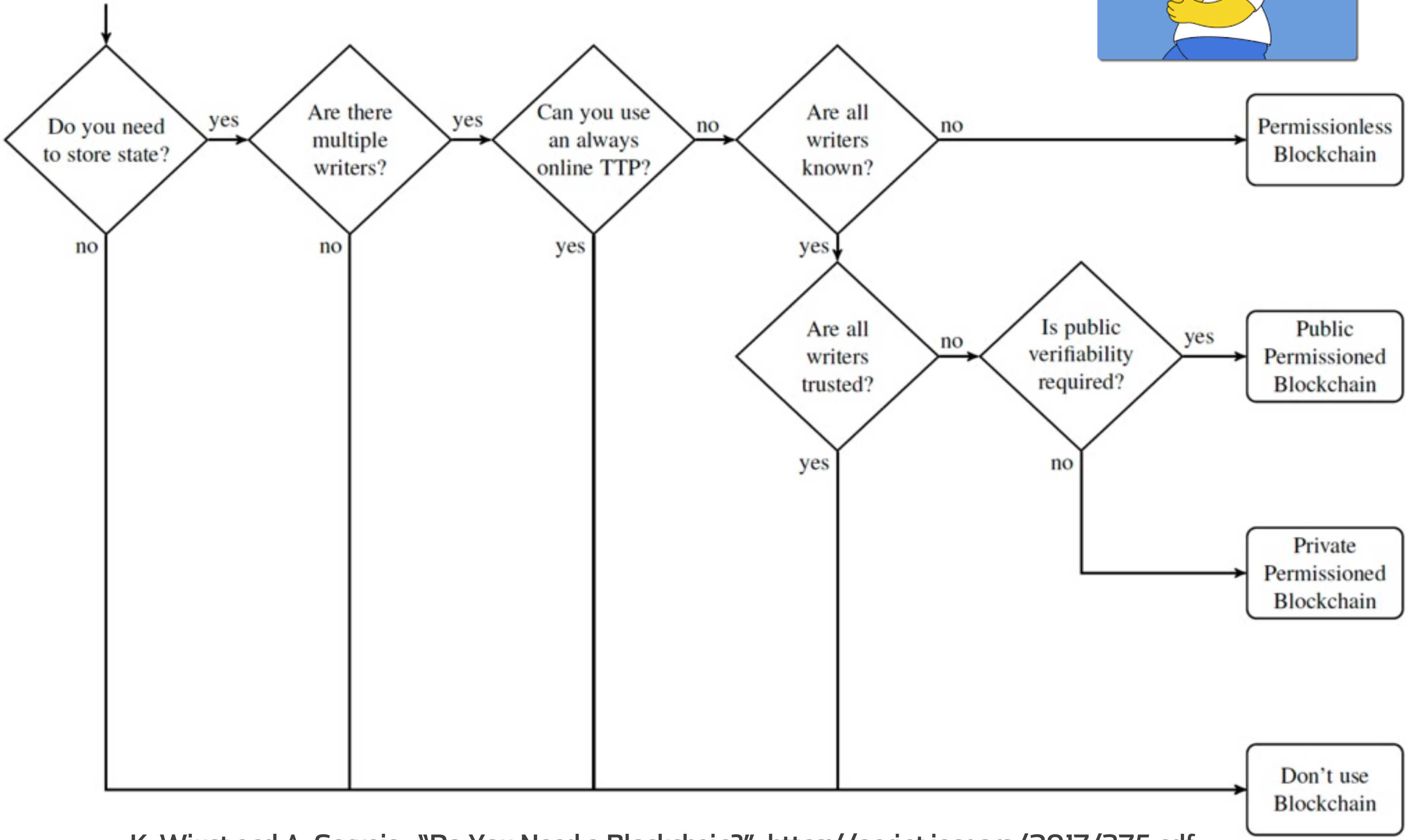
Salient Features

- Distributed Nature
- Chronological and Time stamped Records
- Immutability
- Auditability
- Cryptographically Sealed

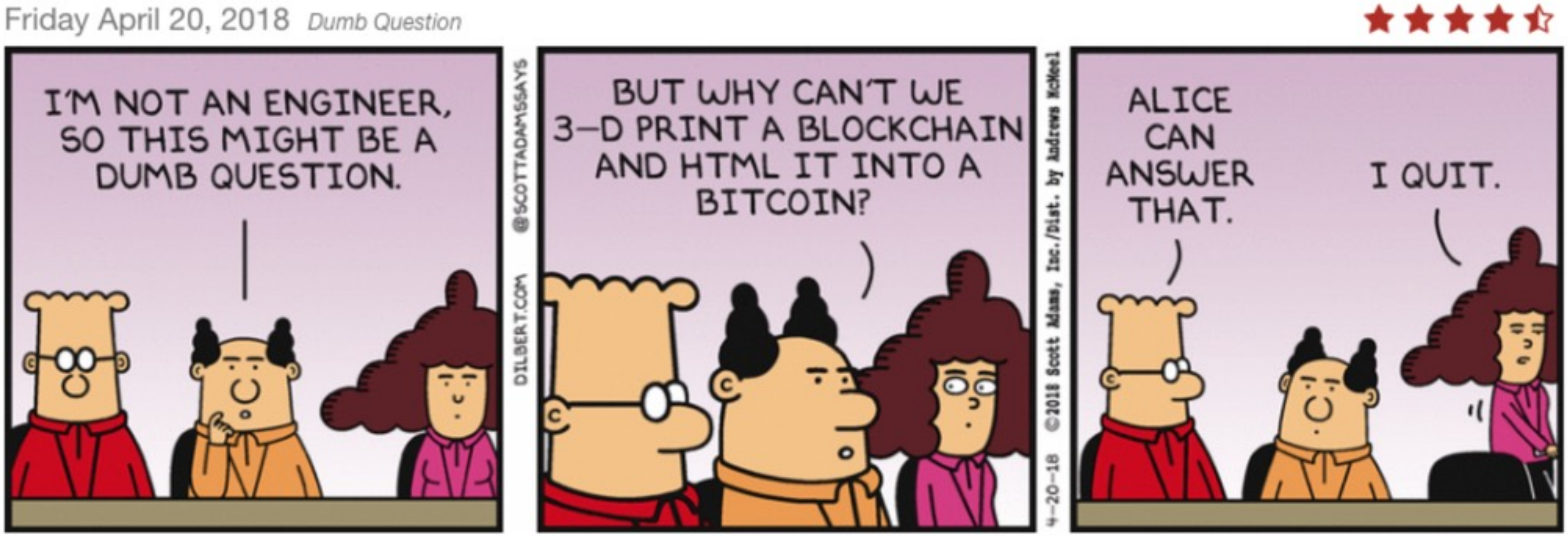
Types of Blockchains

Permissionless	Permissioned
Public	Private / Consortium / Public
Anonymous users	Identified users
Slow	Fast
Proof of work, Proof of stake, Proof of importance, Proof of time-elapsed	PBFT, RAFT, PoET
Examples: Bitcoin, Ethereum, NEM, IOTA	Examples: Hyperledger, R3 (Corda), Ripple, Quorum

So is Blockchain indeed the answer?


Do you need to store state?
yes
no
Are there multiple writers?
yes
no
Can you use an always online TTP?
no
yes
Are all writers known?
no
yes
Permissionless Blockchain
Are all writers trusted?
no
yes
Is public verifiability required?
yes
no
Public Permissioned Blockchain
Private Permissioned Blockchain
Don't use Blockchain

K. Wiust and A. Gervais., "Do You Need a Blockchain?", https://eprint.iacr.org/2017/375.pdf


Friday April 20, 2018 Dumb Question
I'M NOT AN ENGINEER, SO THIS MIGHT BE A DUMB QUESTION.
@SCOTTADAMSSAYS
DILBERT.COM
BUT WHY CAN'T WE 3-D PRINT A BLOCKCHAIN AND HTML IT INTO A BITCOIN?
©2018 Scott Adams, Inc./Dist. by Andrews McMeel
4-20-18
ALICE CAN ANSWER THAT.
I QUIT.

1 Internet of Things

Motivating Example

Motivating Example

BLOCK CHAIN

Challenges of adopting blockchain in IoT

Complex Consensus Algorithms

THAT AWKWARD MOMENT, WHILE WAITING FOR CONFIRMATION OF A TRANSACTION
ANYTIME NOW!
SO, HOW'S THE KIDS?
THE BITCOIN COMIC
BY Z1XWITCH
Special thanks to bitcoinaddict.com
512 × 384

Scale and associated overheads

Latency

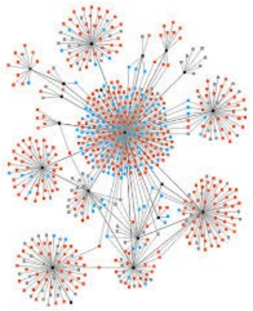
Throughput

Complex security mechanisms (e.g. for preventing double spending) may not be relevant

Incentives

Lightweight Scalable Blockchain (LSB) for IoT

Overlay network comprised of IoT devices, gateways, service provider servers, cloud storage



Nodes organised as clusters and cluster heads responsible for managing the distributed ledger

Number of optimizations to fit the IoT context

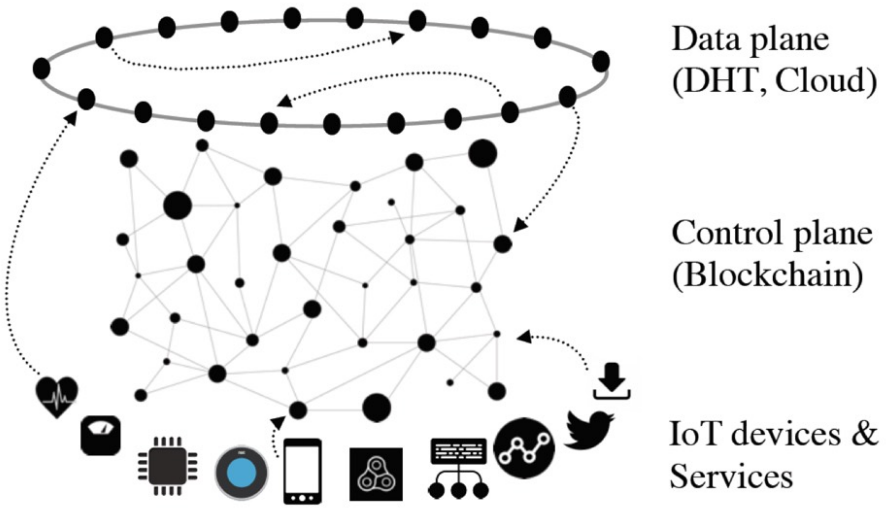
- Distributed time-based consensus
- Distributed trust
- Distributed throughput management

Ali Dorri, Salil S. Kanhere, and Raja Jurdak, "Towards an Optimized BlockChain for IoT", Second IEEE/ACM International Conference on Internet-of-Things Design and Implementation (IoTDI) 2017

Ali Dorri, Salil S. Kanhere, Raja Jurdak and Praveen Gauravaram, "A Lightweight Scalable Blockchain for IoT Security and Privacy", under review, https://arxiv.org/abs/1712.02969

Some fundamental concepts

Separation of transaction traffic and data flow and the data/control plane



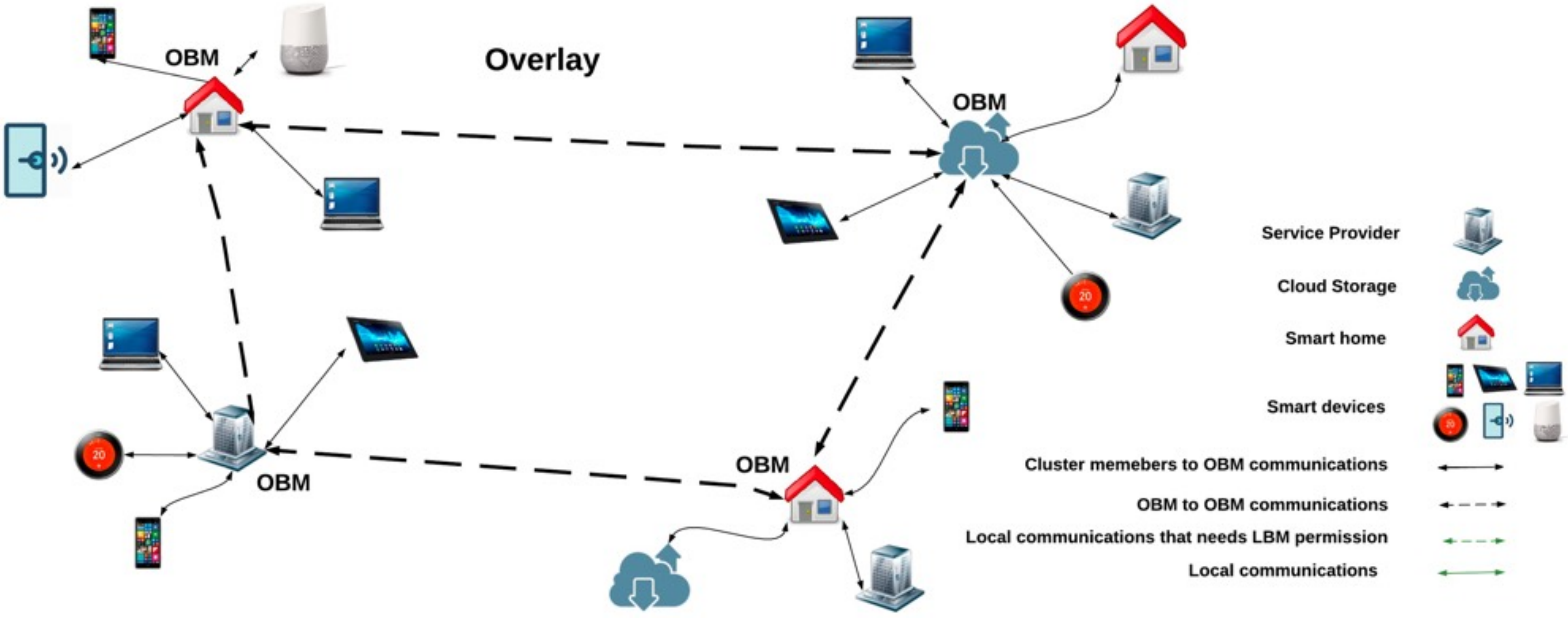
IoT device data is stored **off-the-chain**

- Cloud storage
- Local storage (where relevant)

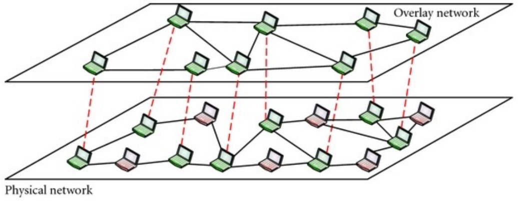
Overlay Block Manager (OBM): Entity responsible for managing the blockchain

- Generation, verification and storage of individual transactions and blocks of transactions
- Access control

LSB Overview


OBM
Overlay
OBM
OBM
OBM
Service Provider
Cloud Storage
Smart home
Smart devices
Cluster memebers to OBM communications
OBM to OBM communications
Local communications that needs LBM permission
Local communications

Overlay



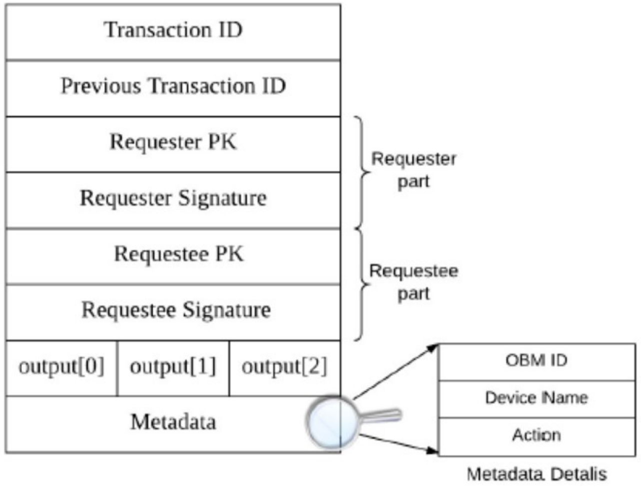
Each node is known by a public key (changeable for anonymity)

Nodes organised as clusters and each cluster elects a cluster head (CH) -> OBM

Transactions are secured using asymmetric encryption, digital signatures and cryptographic hash functions

- Single Signature Transactions
- Multiple Signature Transactions (m out of n)

Separate transaction ledger per node



Limiting Spam Accounts

Genesis transaction created using one of the following approaches:

- Certificate Authorities: Leverages PKI. A CA ratifies the node’s PK which is included in the genesis transaction.

- Burn coin in Bitcoin: A transaction created in the Bitcoin blockchain by destroying a specific amount of coin. The genesis transaction uses the same PK as the burn transaction.

OBMs verify validity in either approach.

Transaction Vocabulary

Genesis: starting point of the ledger

Store: used for storing data in the cloud storage

Access: to request access to stored data

Monitor: to enable real-time access to data from a device

Transaction flow is distinct from data flow

- Transactions are broadcast to all OBMs while data is unicast along optimal routes

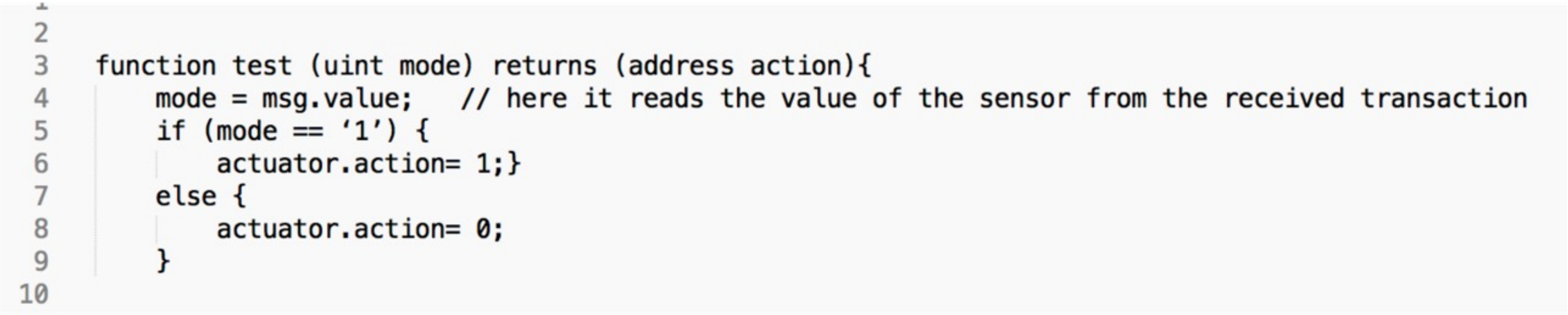
Smart Contracts for D2D Interaction

Manifest **If this then that** interaction

Once mined, the smart contract cannot be modified, thus the participants can trust the contract

Each contract can perform pre-defined actions based on the variables passed to its through transactions

For example:



```

function test (uint mode) returns (address action){
    mode = msg.value;   // here it reads the value of the sensor from the received transaction
    if (mode == ‘1’) {
        actuator.action= 1;}
    else {
        actuator.action= 0;
    }

```

Who can access what?

OBM maintains an Access Control List (ACL) consisting of requester/requestee PK pairs

- Key list updated by cluster members

When a transaction arrives at an OBM, the key list is checked to determine the destination of the transaction

- if the requestee is not part of the OBMs cluster, then the transaction is broadcast to other OBMs

Time-based Consensus

Time-based block generation: One block per consensus-period

A random waiting time before block generation

A new block is broadcast to all other OBMs

Neighbours verify that one block is generated per consensus-period

- Non-compliant blocks are dropped and trust associated with the responsible OBM is decreased

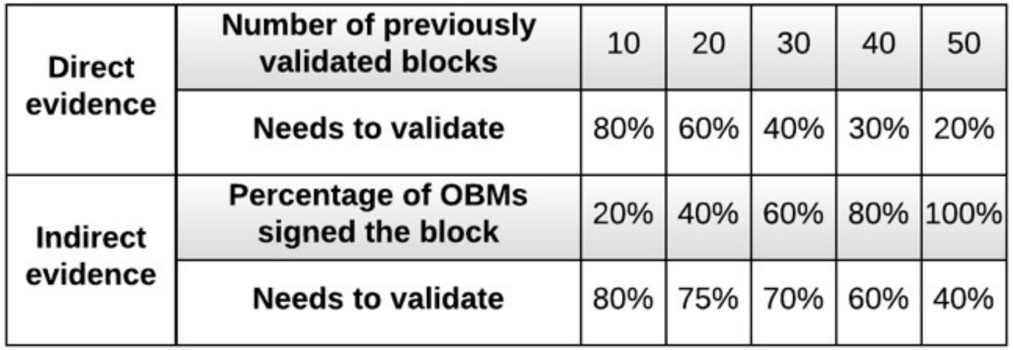
Block Verification

Verifying all transactions in a block is computationally demanding

A portion of the transactions are verified as the OBMs build up trust in one another

Distributed trust

- Direct evidence – if OBM Y has verified a block generated by OBM X
- Indirect evidence – If OBM Z (not Y) has verified the new block generated by OBM X



Direct evidence	Number of previously validated blocks	10	20	30	40	50
	Needs to validate	80%	60%	40%	30%	20%
Indirect evidence	Percentage of OBMs signed the block	20%	40%	60%	80%	100%
	Needs to validate	80%	75%	70%	60%	40%

Distributed Throughput Management

Throughput = average number of transactions appended to the BC per second

Classical consensus algorithms limit the throughput (e.g., Bitcoin throughput is limited to 7 transactions per second)

Measures the utilization **α** (ratio of # of transactions generated to the # of transactions appended) in each consensus period

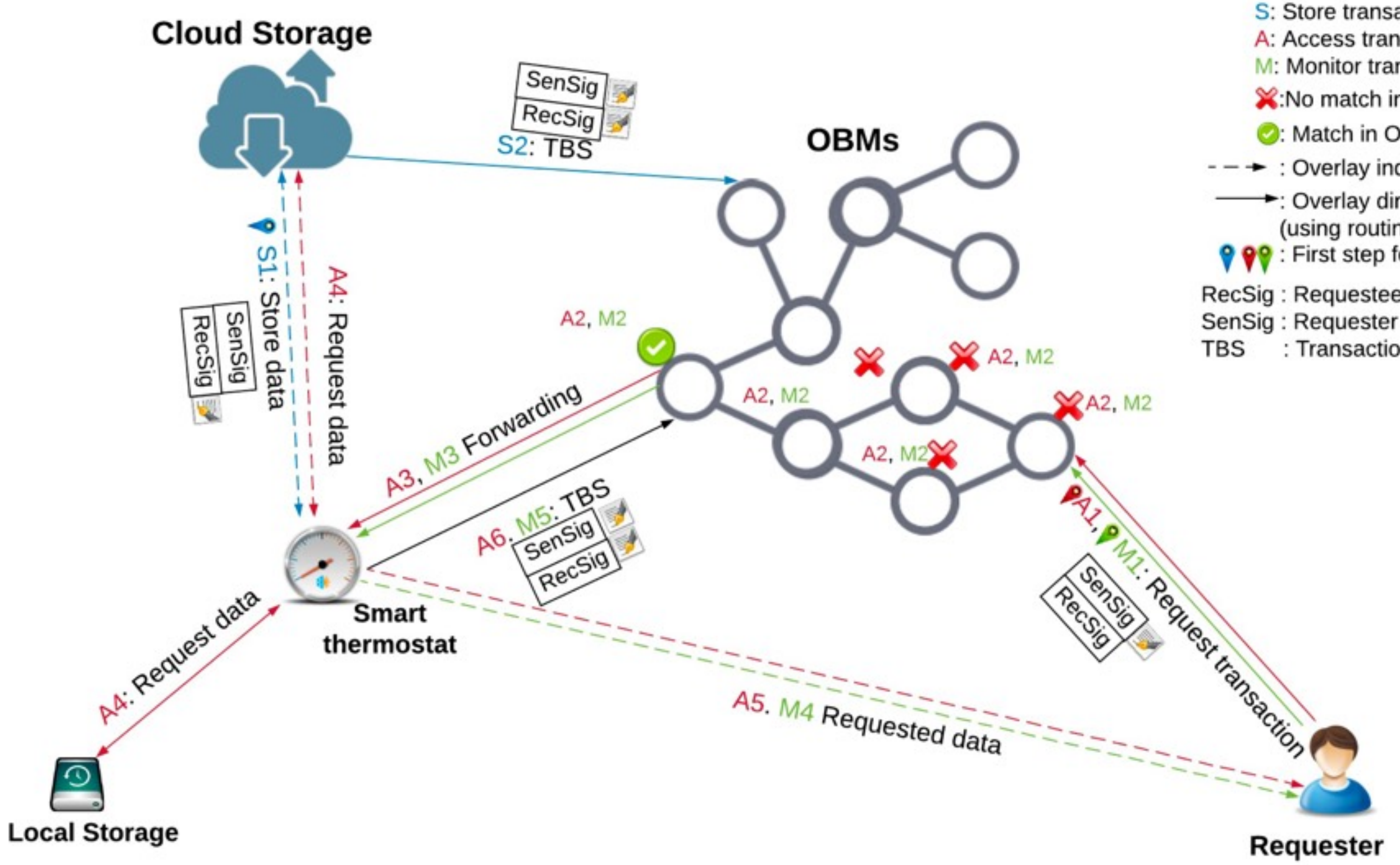
Goal : **α_{min} <= α <= α_{max}**

$$\boxed{\alpha = \frac{N * R * Consensus-period}{T\_max * M}}$$

Tune two parameters to guarantee the above condition

- Consensus-period
- The number of OBMs (M)

Transaction Flow



S: Store transaction

A: Access transaction

M: Monitor transaction

✗:No match in OBM key lists

✓: Match in OBM key lists

- - → : Overlay indirect communications

→: Overlay direct communications (using routing protocols)

● ● ●: First step for each transaction

RecSig	: Requestee signature
SenSig	: Requester signature
TBS	: Transaction to be stored on BC

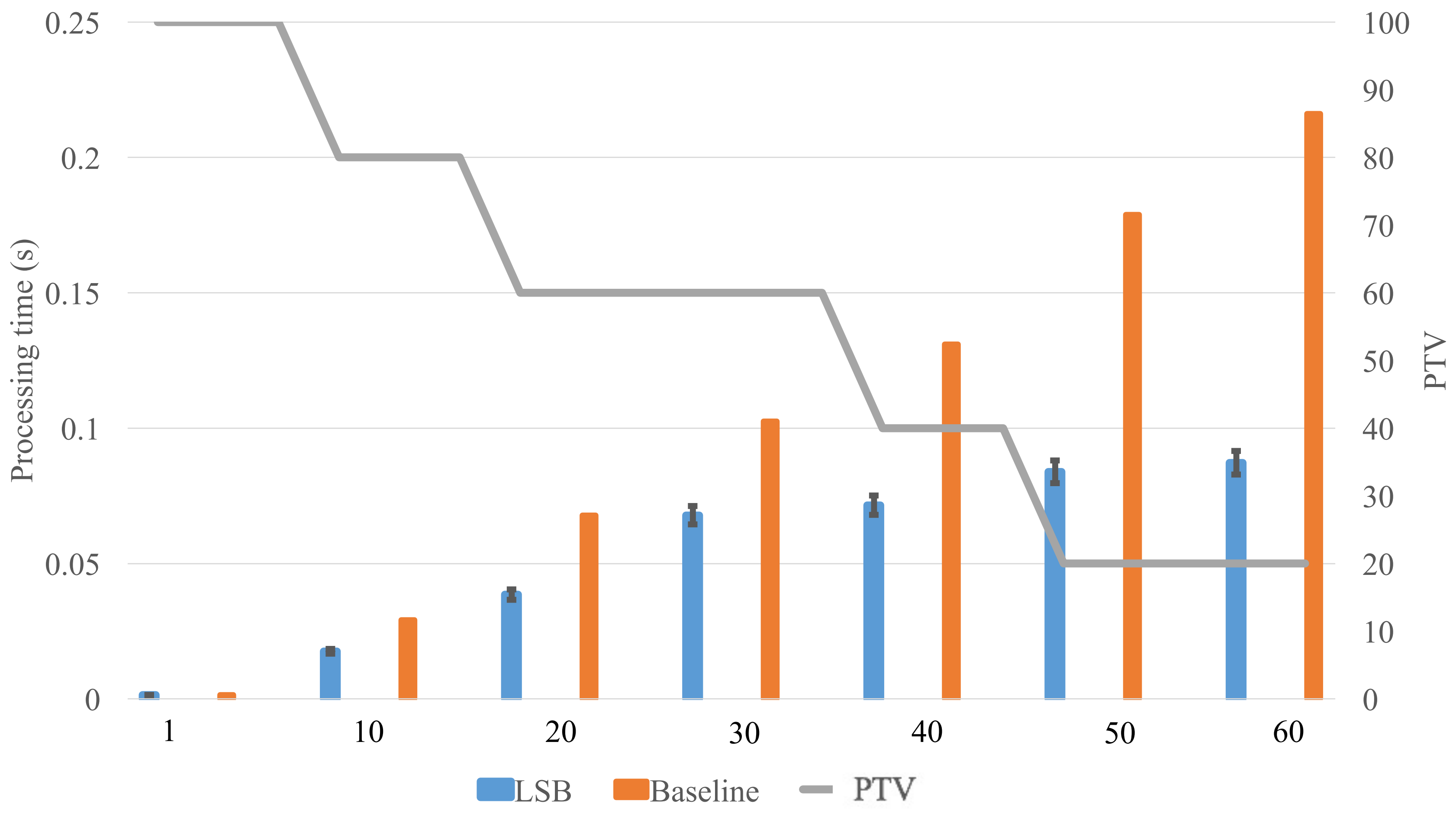
Security Analysis

Requirement	Employed method
Confidentiality	Encryption can be used for the data
Integrity	Each transaction includes a hash of all other fields contained in the transaction
Availability	An OBM sends a transaction to its cluster members only if a key contained in the transaction matches one of the entries in its keylist. This ensures that the cluster members only receive transactions from authorized nodes.
Authentication	Each node should have a stored genesis transaction in the BC to be authenticated. As transactions are chained to the genesis transaction, a node is authenticated when it has the private key corresponding to the output PK of a transaction stored in the BC
Non-repudiation	Transactions are signed by the transaction generator to achieve non-repudiation. Additionally, all transactions are stored in the BC, so involved parties in the transaction can deny their complicity in a transaction

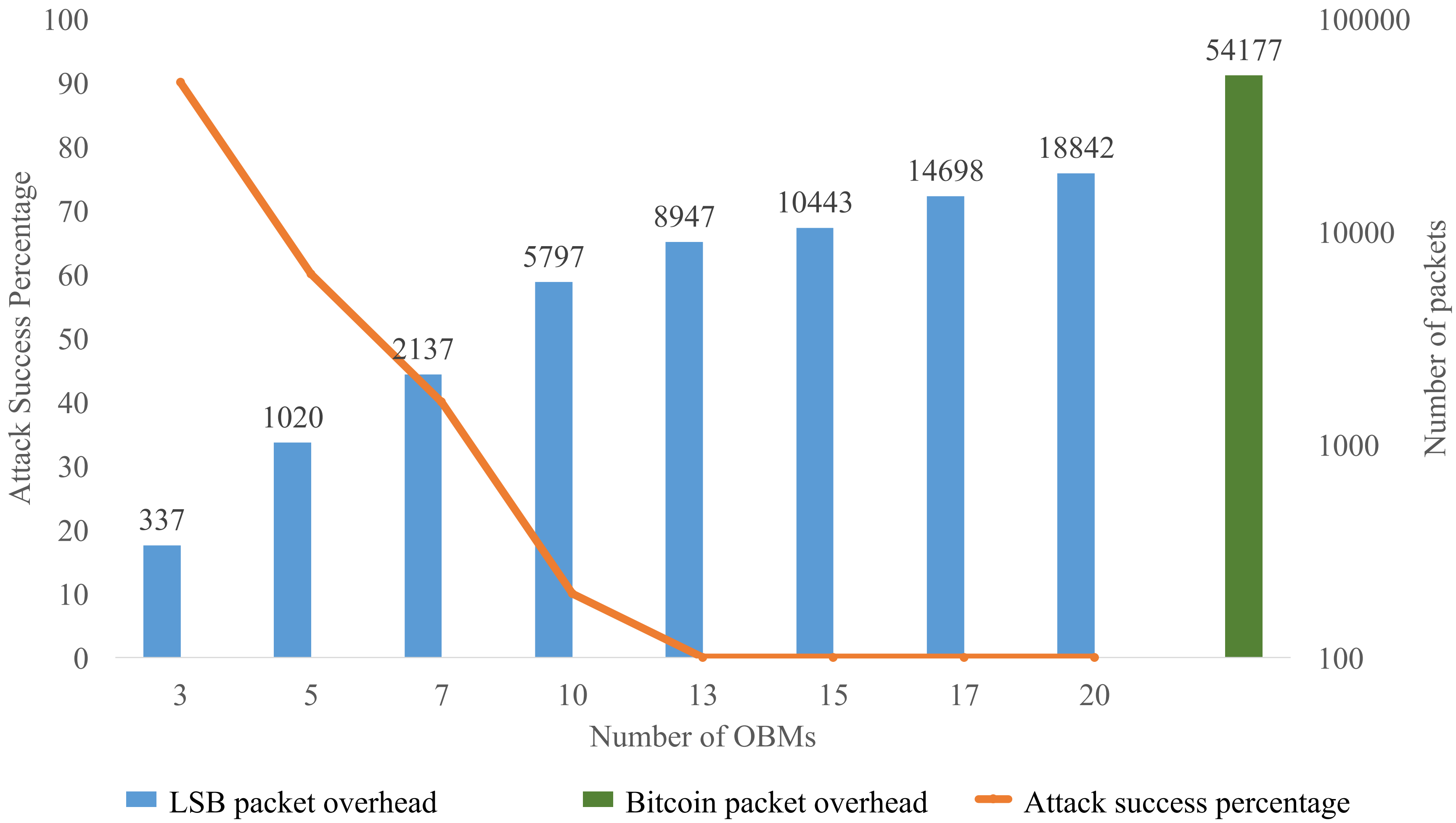
Performance Evaluation

- Simulations:
  - Smart home tier:
    - Cooja Simulator
    - 6LoWPAN
    - Focus on overheads incurred by the CC
  - Overlay tier:
    - Ns3 Simulator
    - 50 node overlay network with 13 OBMS (default), 5 requesters generating 4 transactions per second

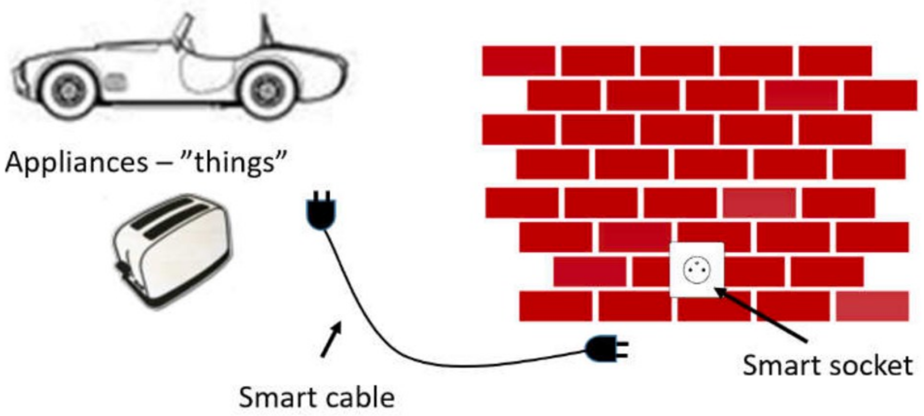
Distributed Trust

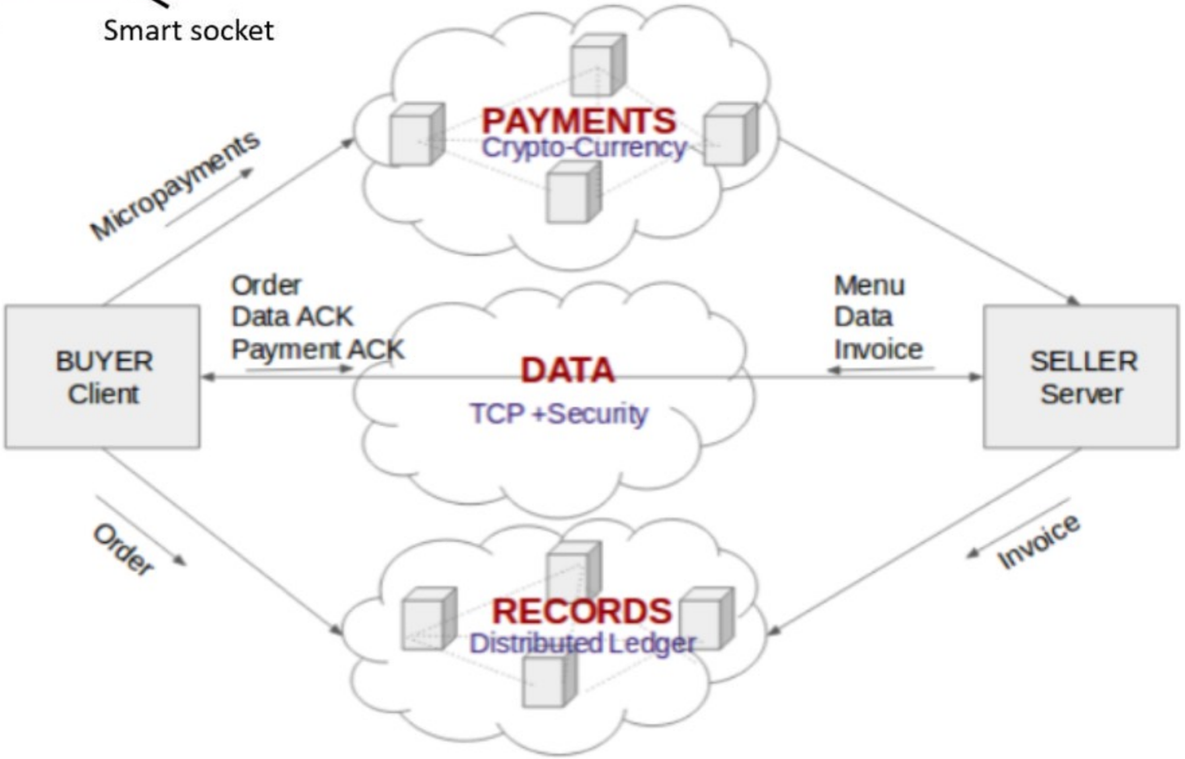


Resilience to Attacks



IoT Data/Service Marketplace

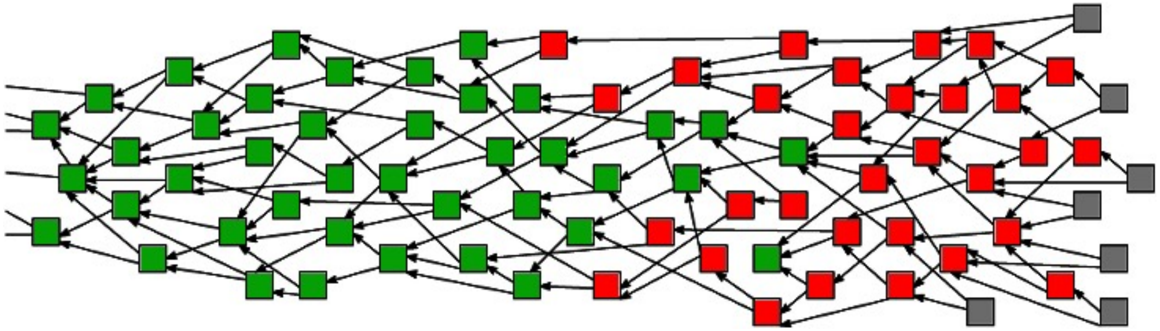




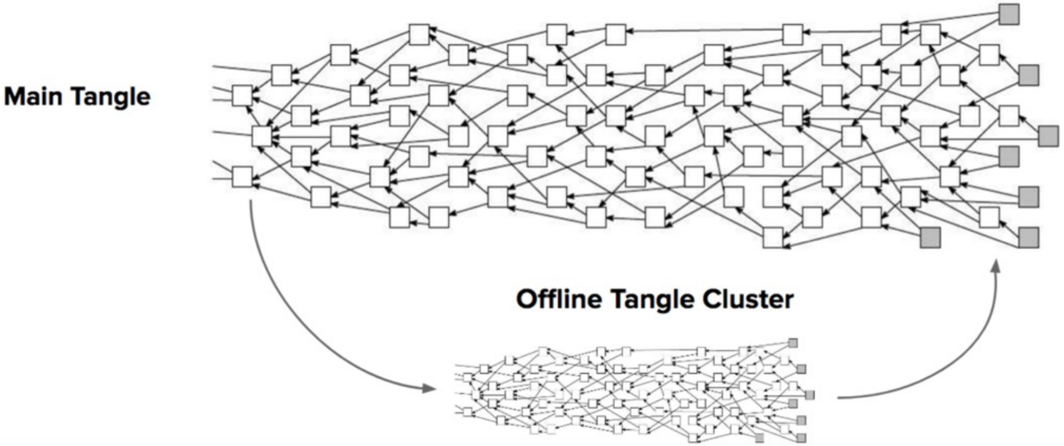
IOTA

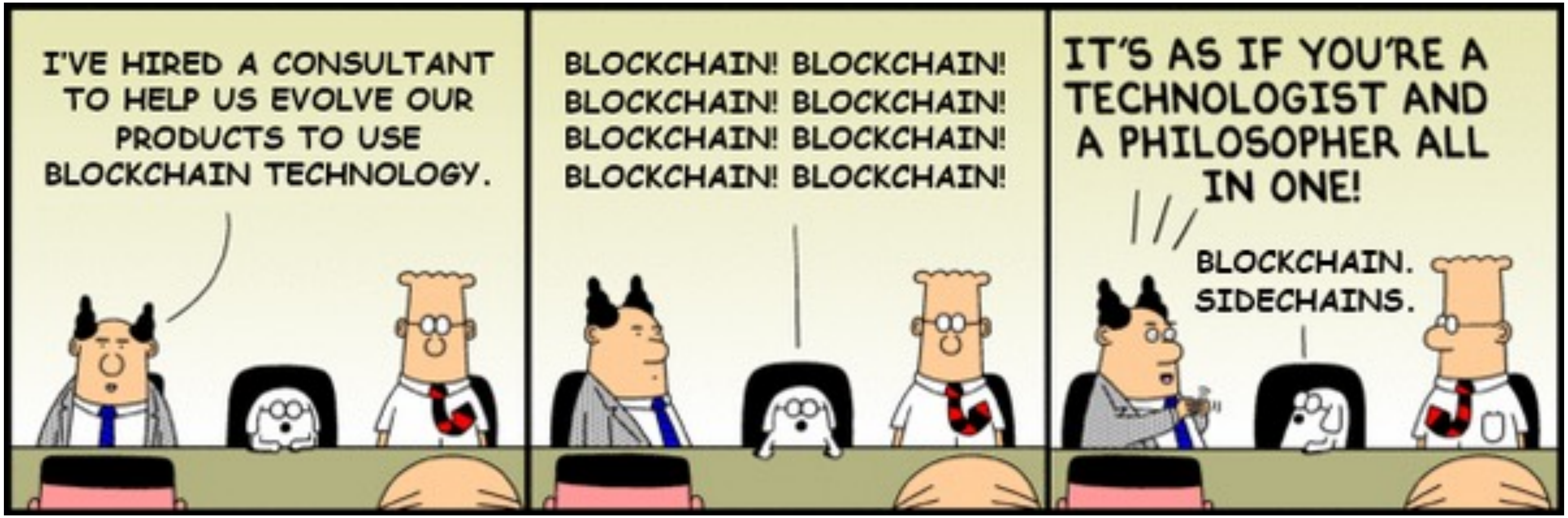
A Blockchain **without the Blocks** and the **Chain**

Tangle



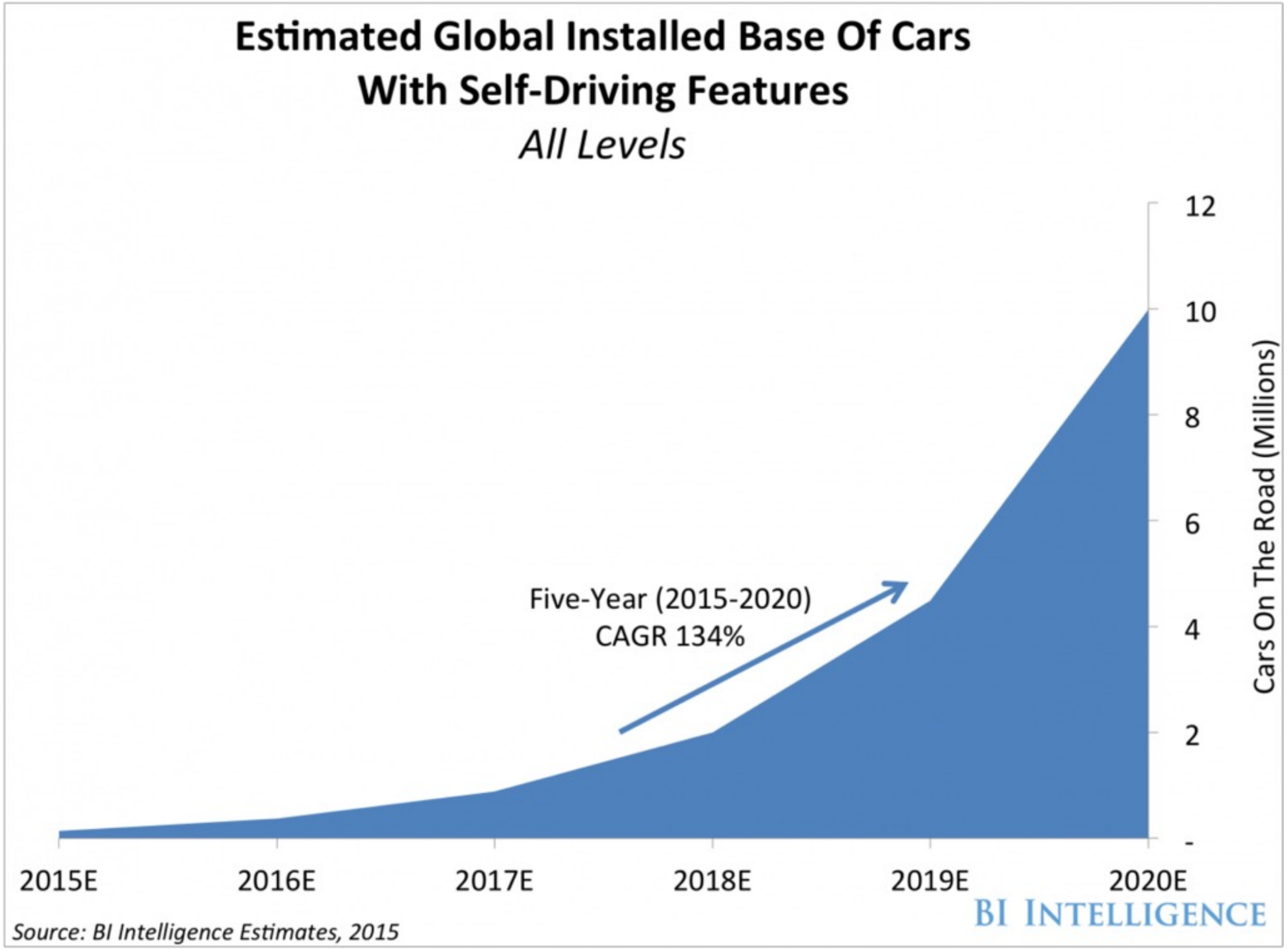
- All transactions bundled in a Directed Acyclic Graph (DAG)
- Each new transaction must approve two previous transactions
- PoW for preventing spam
- Flexibility in “confirming” transactions
- No transaction fees
- Support for offline transactions (partitioning)




I'VE HIRED A CONSULTANT TO HELP US EVOLVE OUR PRODUCTS TO USE BLOCKCHAIN TECHNOLOGY.
BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN! BLOCKCHAIN!
IT'S AS IF YOU'RE A TECHNOLOGIST AND A PHILOSOPHER ALL IN ONE!
BLOCKCHAIN. SIDECHAINS.

2 CONNECTED VEHICLES

Connected and Automated Vehicles



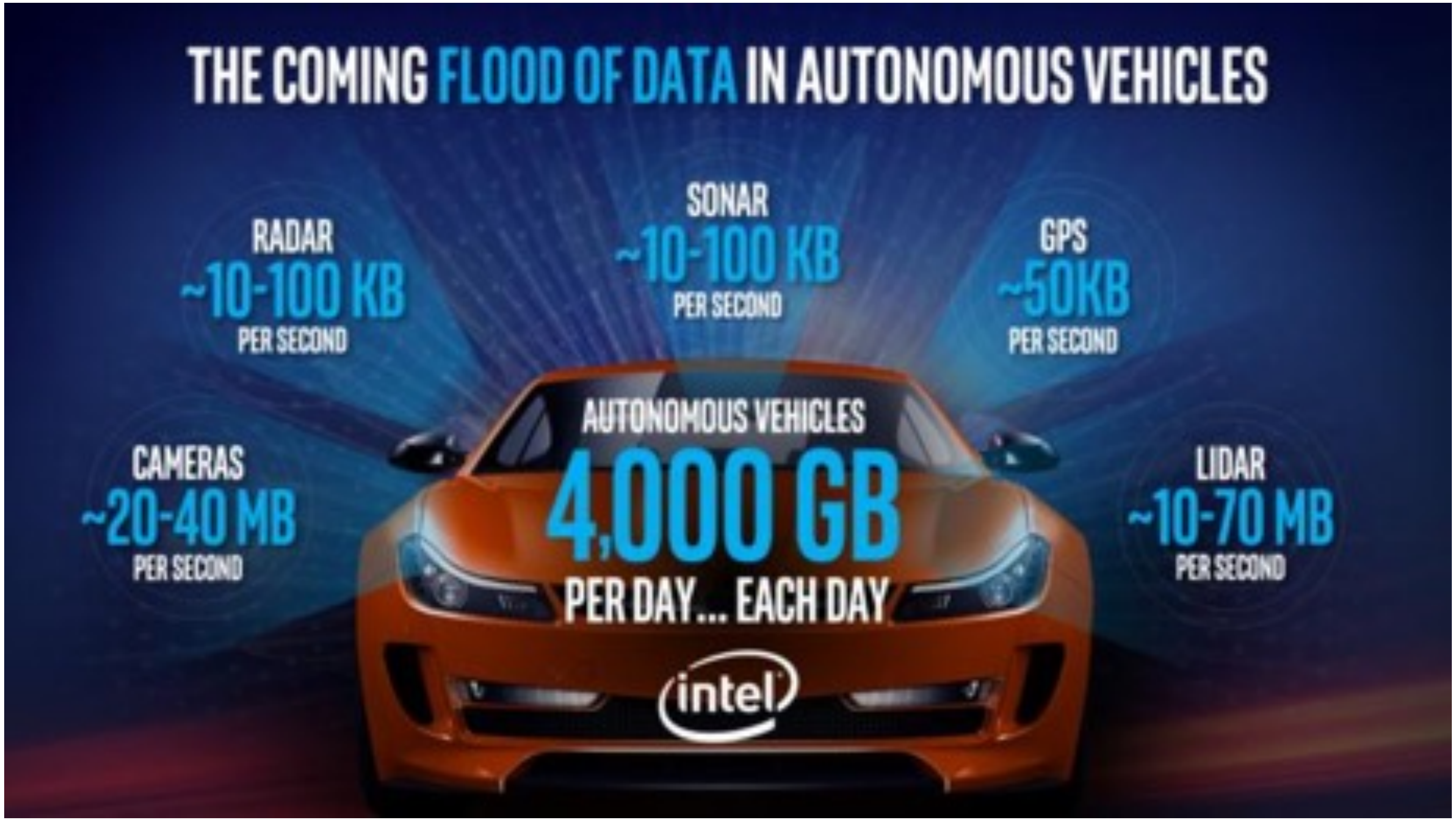
Estimated Global Installed Base Of Cars With Self-Driving Features

All Levels

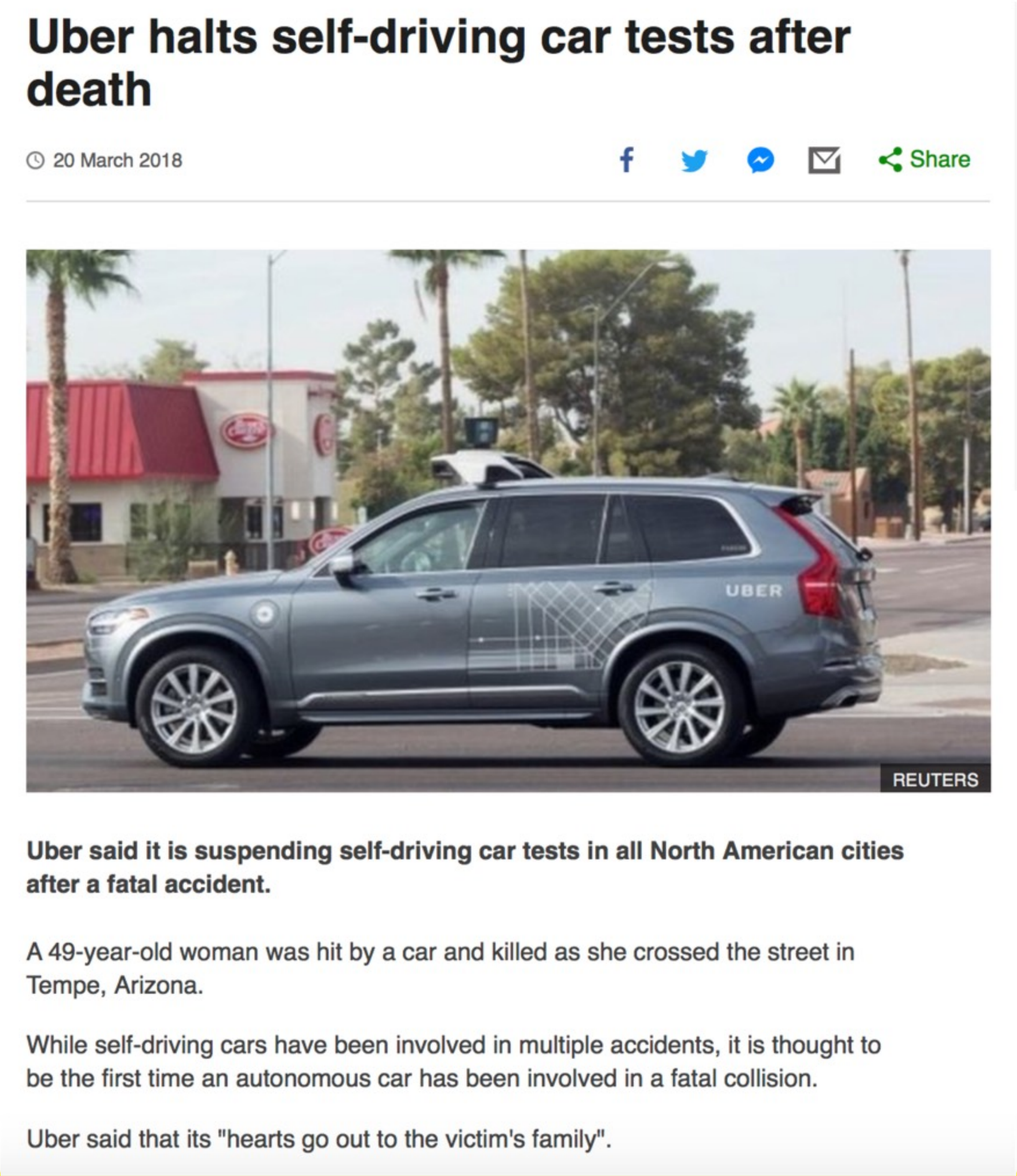
Five-Year (2015-2020) CAGR 134%

Source: BI Intelligence Estimates, 2015

Connected and Automated Vehicles



Wide array of ECUs, sensors and connected technologies for better perception of the environment and facilitate independent decision making



Uber halts self-driving car tests after death

20 March 2018

REUTERS

Uber said it is suspending self-driving car tests in all North American cities after a fatal accident.

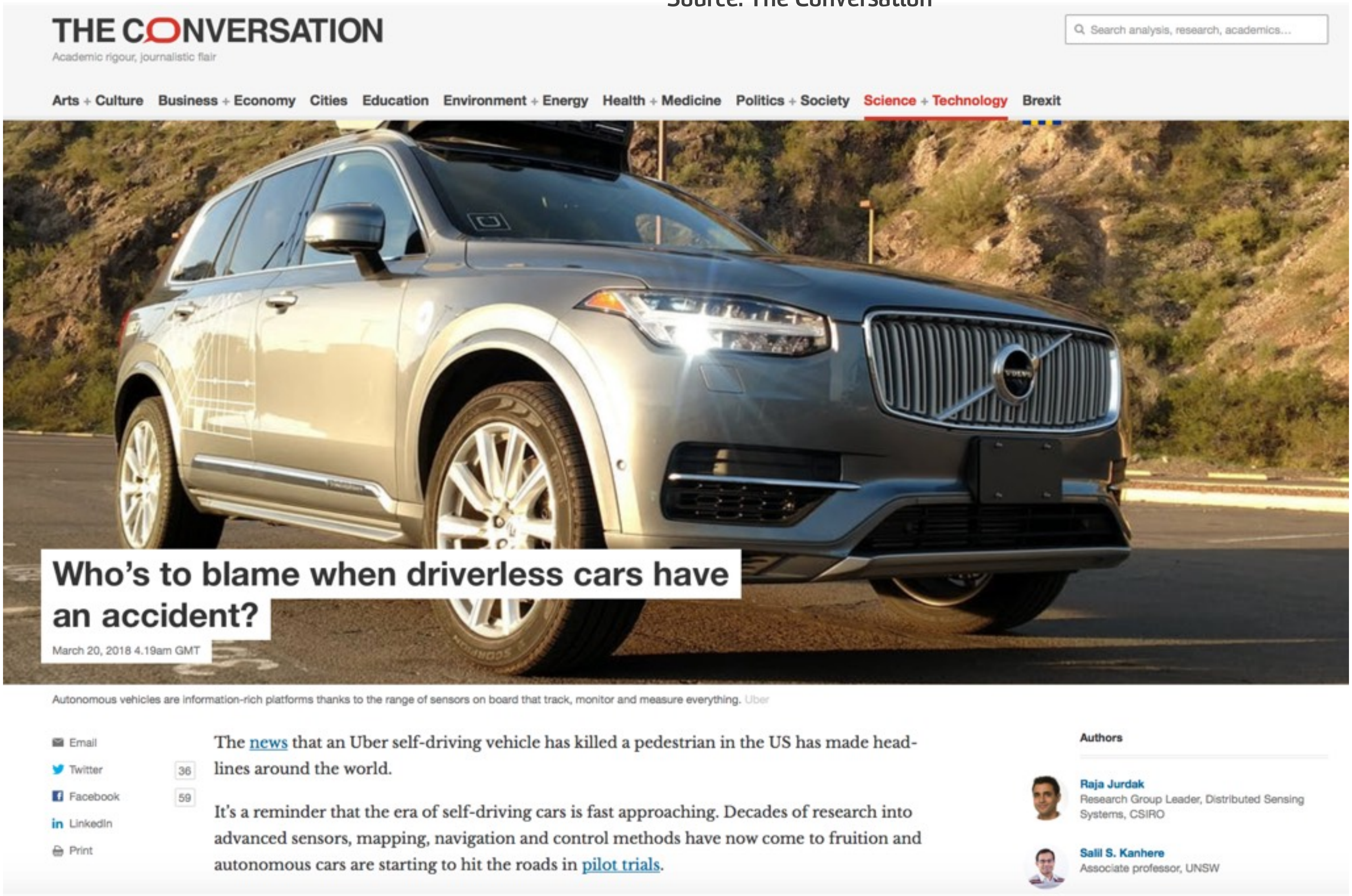
A 49-year-old woman was hit by a car and killed as she crossed the street in Tempe, Arizona.

While self-driving cars have been involved in multiple accidents, it is thought to be the first time an autonomous car has been involved in a fatal collision.

Uber said that its "hearts go out to the victim's family".

Source: BBC

Source: The Conversation



THE CONVERSATION

Academic rigour, journalistic flair

Who's to blame when driverless cars have an accident?

March 20, 2018 4.19am GMT

Autonomous vehicles are information-rich platforms thanks to the range of sensors on board that track, monitor and measure everything. Uber

The news that an Uber self-driving vehicle has killed a pedestrian in the US has made headlines around the world.

It's a reminder that the era of self-driving cars is fast approaching. Decades of research into advanced sensors, mapping, navigation and control methods have now come to fruition and autonomous cars are starting to hit the roads in pilot trials.

Authors

Raja Jurdak
Research Group Leader, Distributed Sensing Systems, CSIRO

Salil S. Kanhere
Associate professor, UNSW

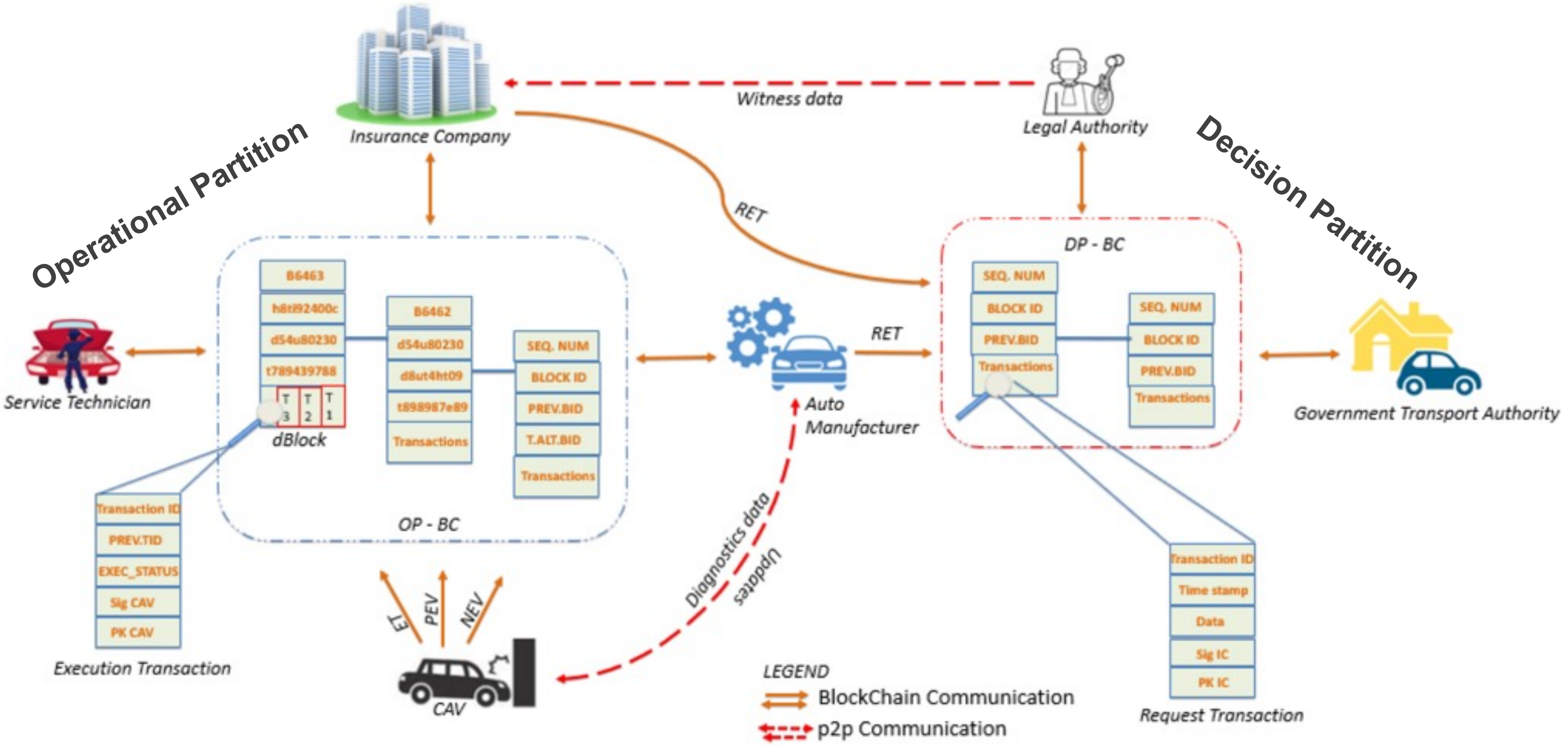
Liability Attribution is Complex

- Product Liability: blame is assigned to an auto manufacturer for product defect
- Service Liability: identified last action of a service technician caused the accident
- Negligence Liability: vehicle owner failed to adhere to instructions and is responsible

Norton Rose Fullbright, Autonomous Vehicles: The Legal Landscape of Dedicated Short Range Communication in the US, UK and Germany, July 2017.

Blockchain Framework for Insurance Claims and Adjudication (B-FICA)

C. Oham, S. S. Kanhere, R. Jurdak and S. Jha, A Blockchain Based Liability Attribution Framework for Autonomous Vehicles, under review, https://arxiv.org/abs/1802.05050



Operational Partition

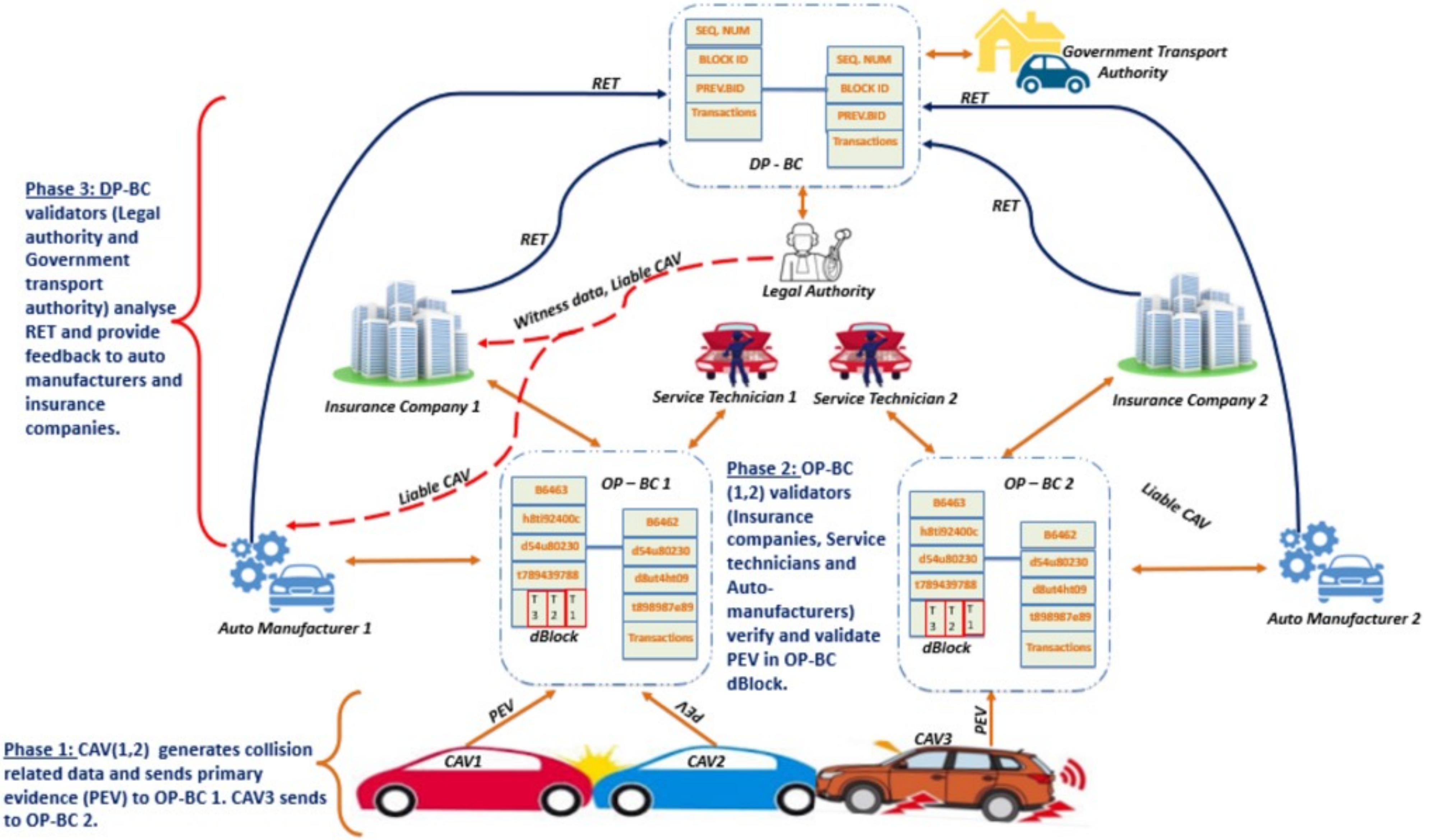
Decision Partition

Transaction Vocabulary

- Event Safety Evidence (ESE): records unexpected vehicular behavior
- Primary Evidence Transaction (PET): records data describing the accident
- Notification Evidence Transaction (NET): records interaction between manufacturer/service technician with CAV
- Execution Transaction (ET): records the CAV’s response to NET
- Request Transaction (RT): for requesting specific data for further investigation

C. Oham, R. Jurdak, S. S. Kanhere, A. Dorri and S. Jha, B-FICA: BlockChain based Framework for auto-Insurance Claim and Adjudication, under review,

Illustrative Example: Two Car Collision

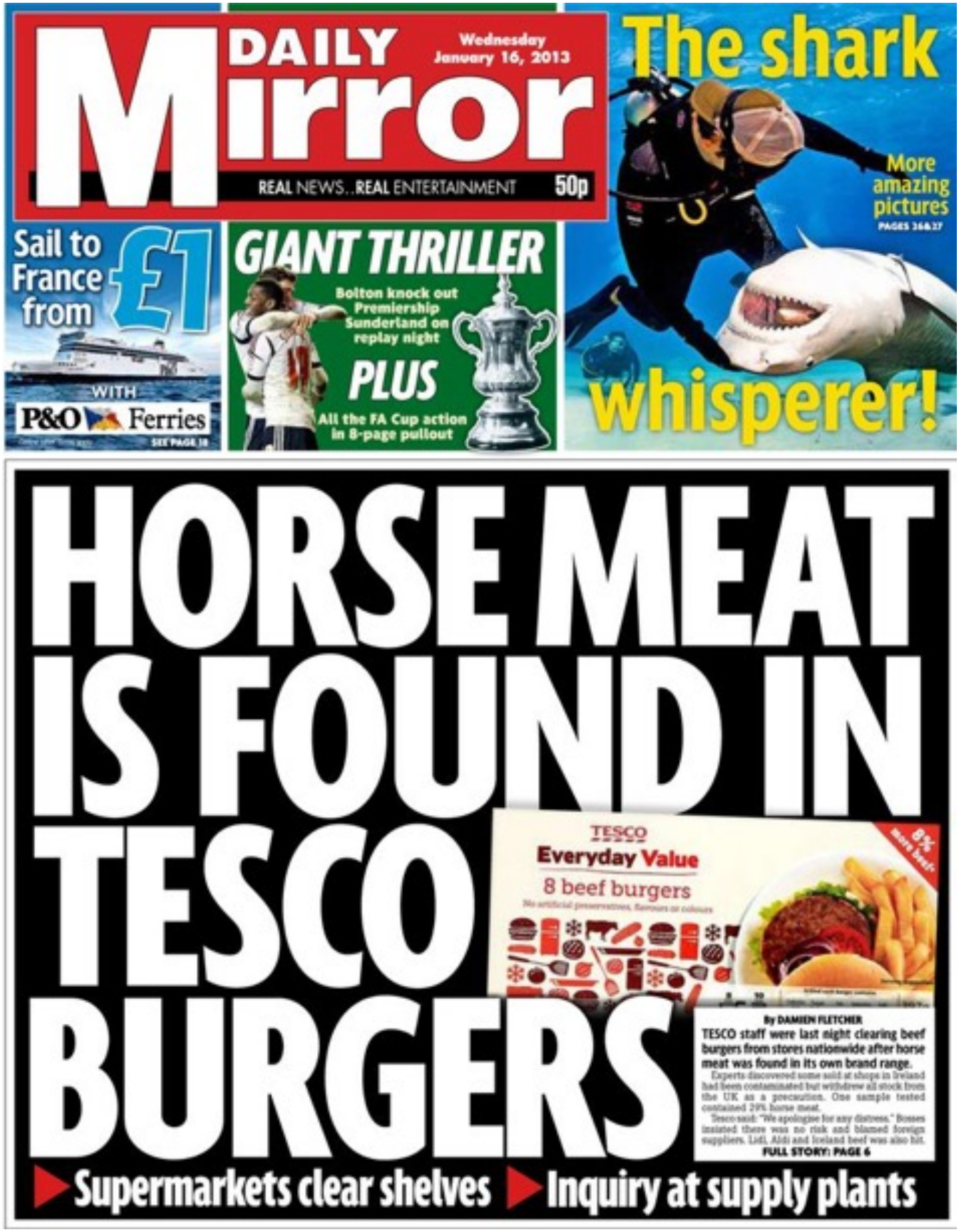


Phase 3: DP-BC validators (Legal authority and Government transport authority) analyse RET and provide feedback to auto manufacturers and insurance companies.

Phase 2: OP-BC (1,2) validators (Insurance companies, Service technicians and Auto-manufacturers) verify and validate PEV in OP-BC dBlock.

Phase 1: CAV(1,2) generates collision related data and sends primary evidence (PEV) to OP-BC 1. CAV3 sends to OP-BC 2.

3 SUPPLY CHAINS



DAILY Mirror

Wednesday
January 16, 2013

REAL NEWS...REAL ENTERTAINMENT 50p

GIANT THRILLER

Bolton knock out Premiership Sunderland on replay night

PLUS

All the FA Cup action in 8-page pullout

The shark whisperer!

More amazing pictures

PAGES 26&27

HORSE MEAT IS FOUND IN TESCO BURGERS

By DAMIEN FLETCHER

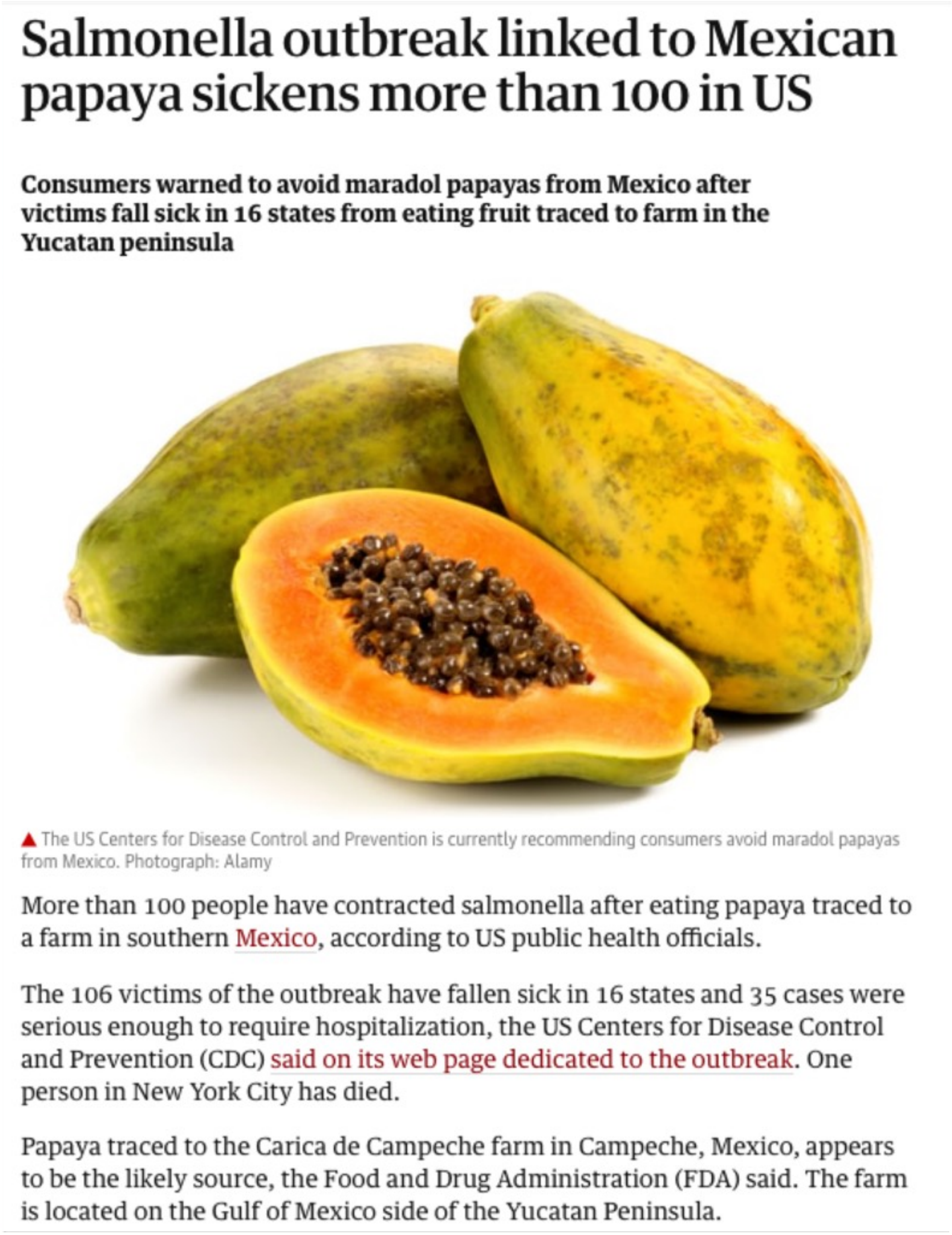
TESCO staff were last night clearing beef burgers from stores nationwide after horse meat was found in its own brand range.

Experts discovered some sold at shops in Ireland had been contaminated but withdrew all stock from the UK as a precaution. One sample tested contained 29% horse meat.

Tesco said: "We apologise for any distress." Bosses insisted there was no risk and blamed foreign suppliers. Lidl, Aldi and Iceland beef was also hit.

FULL STORY: PAGE 6

▶ Supermarkets clear shelves ▶ Inquiry at supply plants



Salmonella outbreak linked to Mexican papaya sickens more than 100 in US

Consumers warned to avoid maradol papayas from Mexico after victims fall sick in 16 states from eating fruit traced to farm in the Yucatan peninsula

▲ The US Centers for Disease Control and Prevention is currently recommending consumers avoid maradol papayas from Mexico. Photograph: Alamy

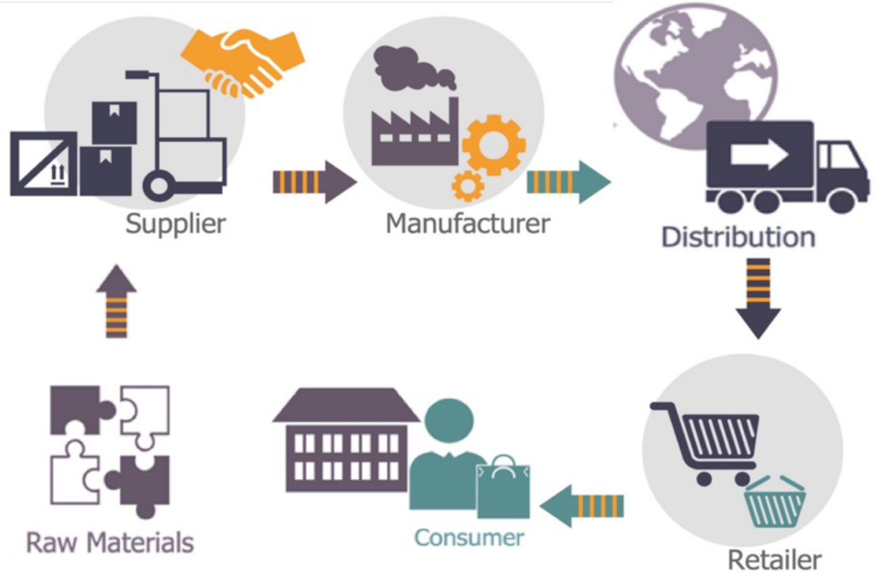
More than 100 people have contracted salmonella after eating papaya traced to a farm in southern Mexico, according to US public health officials.

The 106 victims of the outbreak have fallen sick in 16 states and 35 cases were serious enough to require hospitalization, the US Centers for Disease Control and Prevention (CDC) said on its web page dedicated to the outbreak. One person in New York City has died.

Papaya traced to the Carica de Campeche farm in Campeche, Mexico, appears to be the likely source, the Food and Drug Administration (FDA) said. The farm is located on the Gulf of Mexico side of the Yucatan Peninsula.

Supply Chains

- A system of organizations, people activities, involved in the distribution of raw material or finished goods
  - Food
  - Pharmaceutical
  - Aerospace and Defense



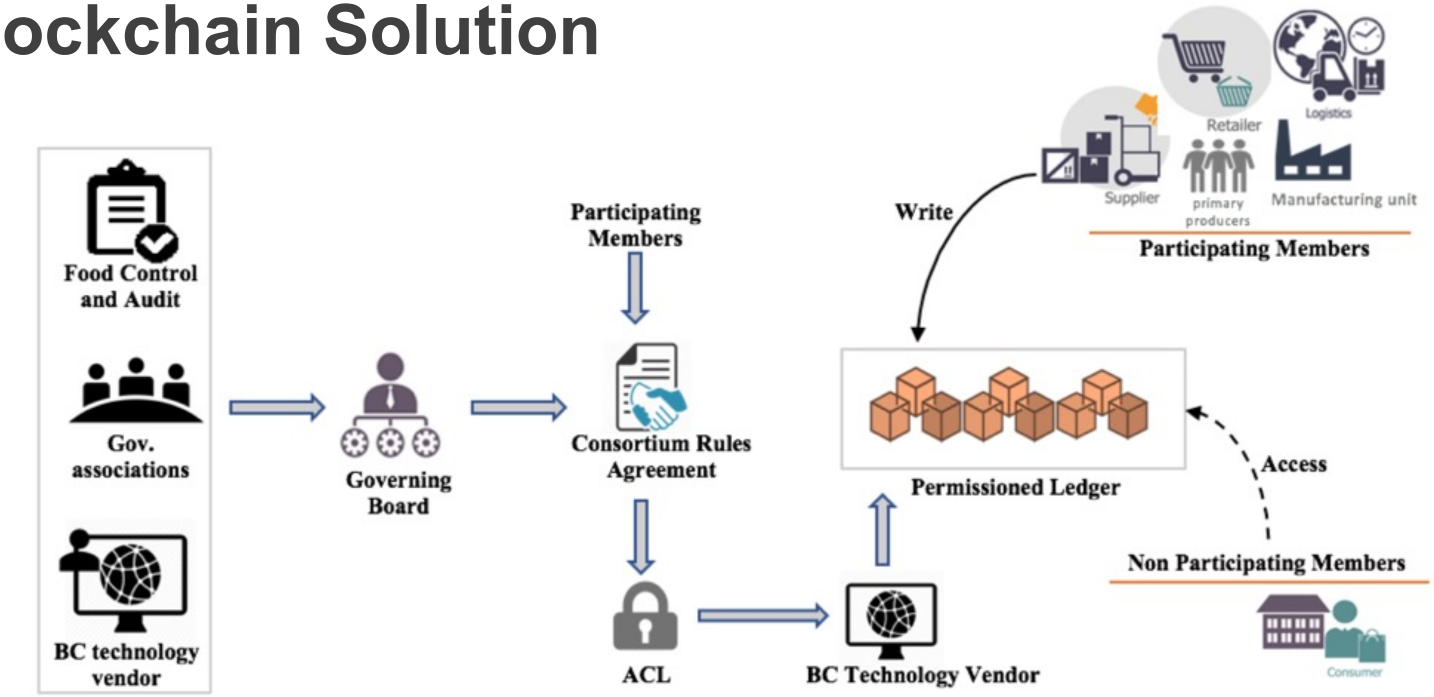
- State-of-the-art traceability systems
  - Organisational silos
  - Prone to mishandling, counterfeiting
  - Consumer access to data often not available or incomplete

Product Story: Necessitates data collection from these repositories and to ensure integrity of data

How can a blockchain help?

- Origin of raw materials can be recorded
- Physical handover of items along the FSC can be tracked
- IoT sensor data streams can be integrated
- Hazard Analysis and Critical Control Points (HAACP) verification can be achieved
- Customers can access product story
- Speed up investigation of sickness outbreaks

A Blockchain Solution



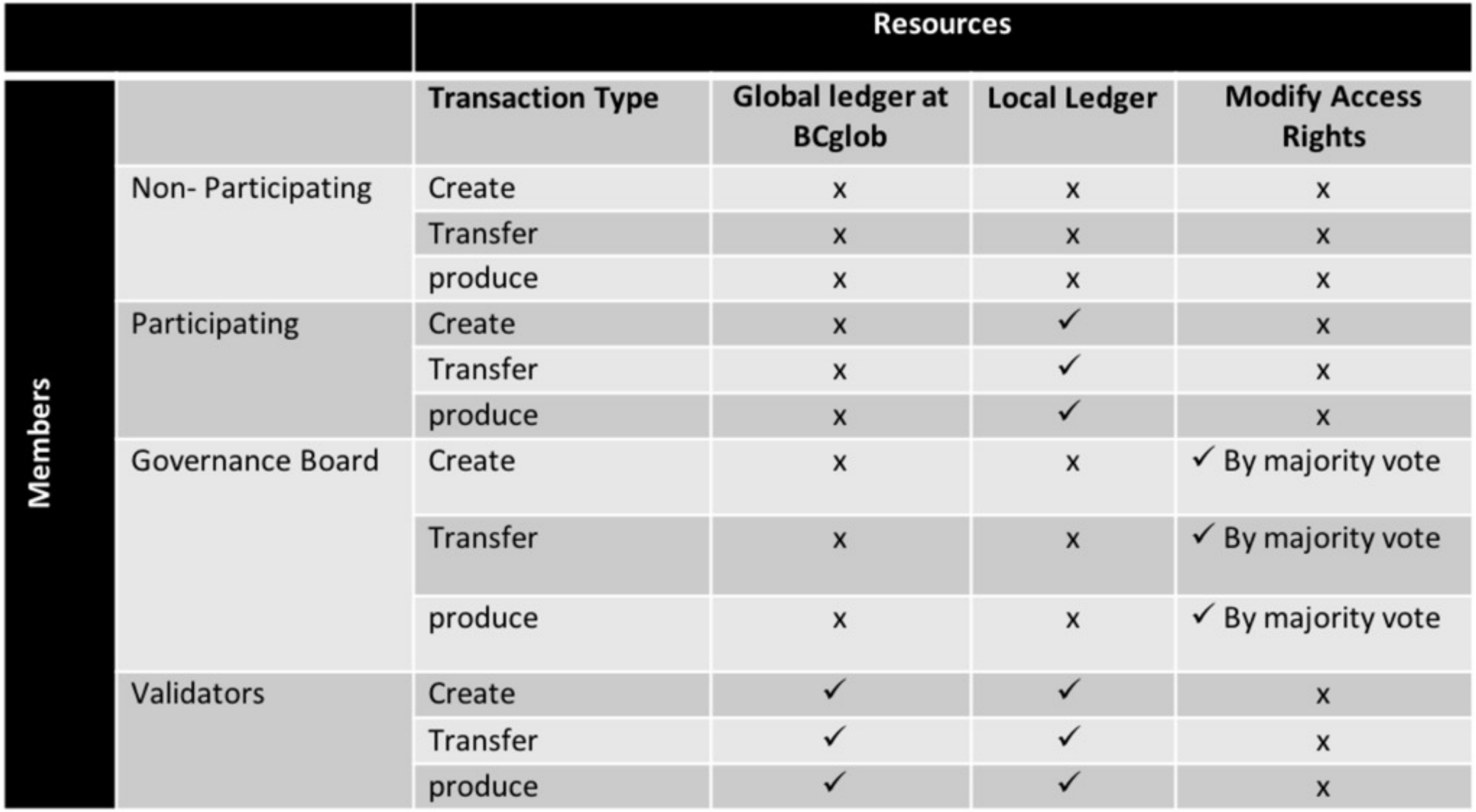
Consortium Blockchain

Governance Board

- Access Control

S. Malik, S. S. Kanhere and R. Jurdak, “Blockchain for Transparent Food Supply Chains”, under review

Access Control



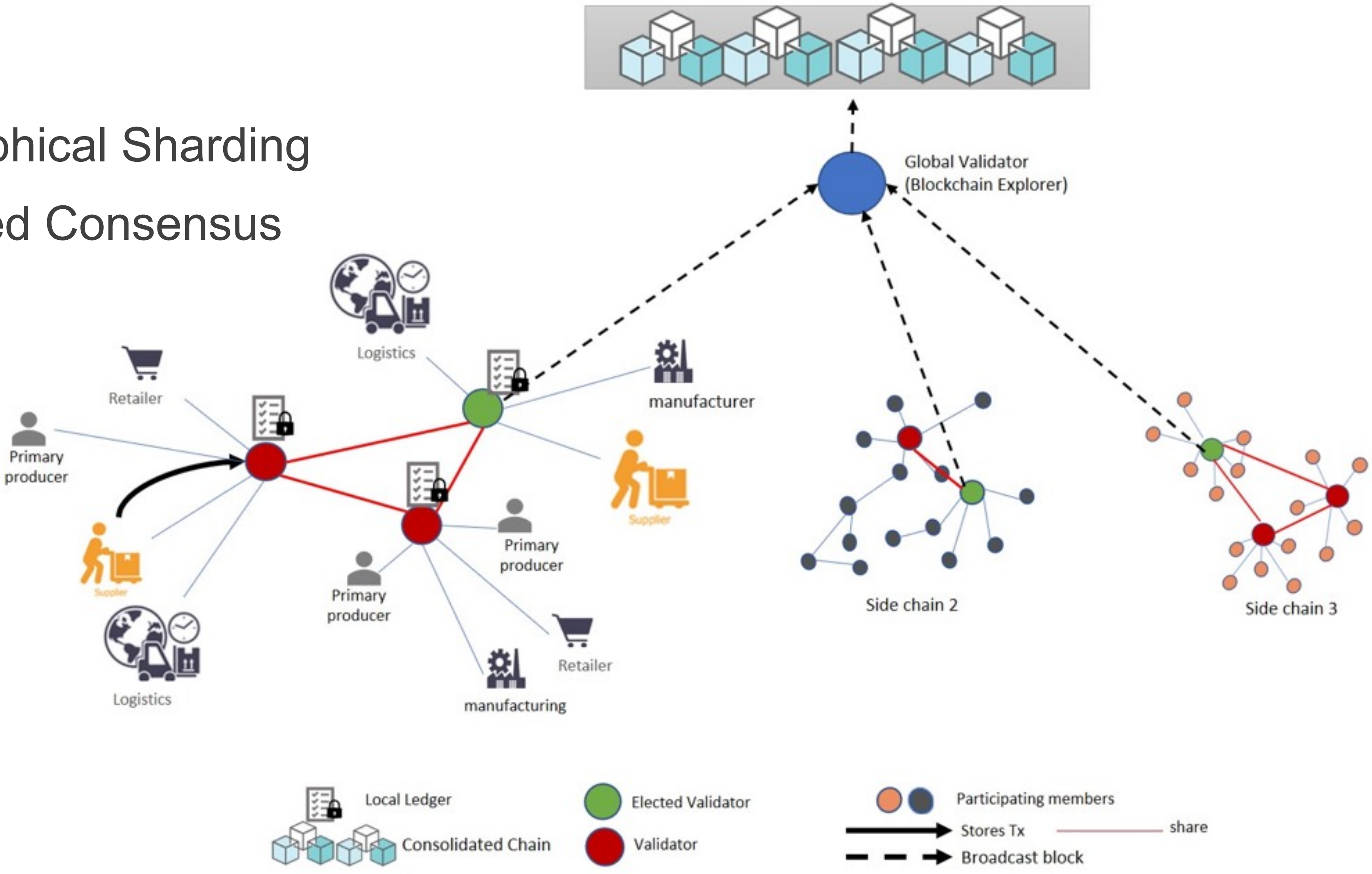
		Resources			
Members		Transaction Type	Global ledger at BCglob	Local Ledger	Modify Access Rights
	Non- Participating	Create	x	x	x
		Transfer	x	x	x
		produce	x	x	x
	Participating	Create	x	✓	x
		Transfer	x	✓	x
		produce	x	✓	x
	Governance Board	Create	x	x	✓ By majority vote
		Transfer	x	x	✓ By majority vote
		produce	x	x	✓ By majority vote
	Validators	Create	✓	✓	x
		Transfer	✓	✓	x
		produce	✓	✓	x

Tiered Network Architecture

3 Tiers

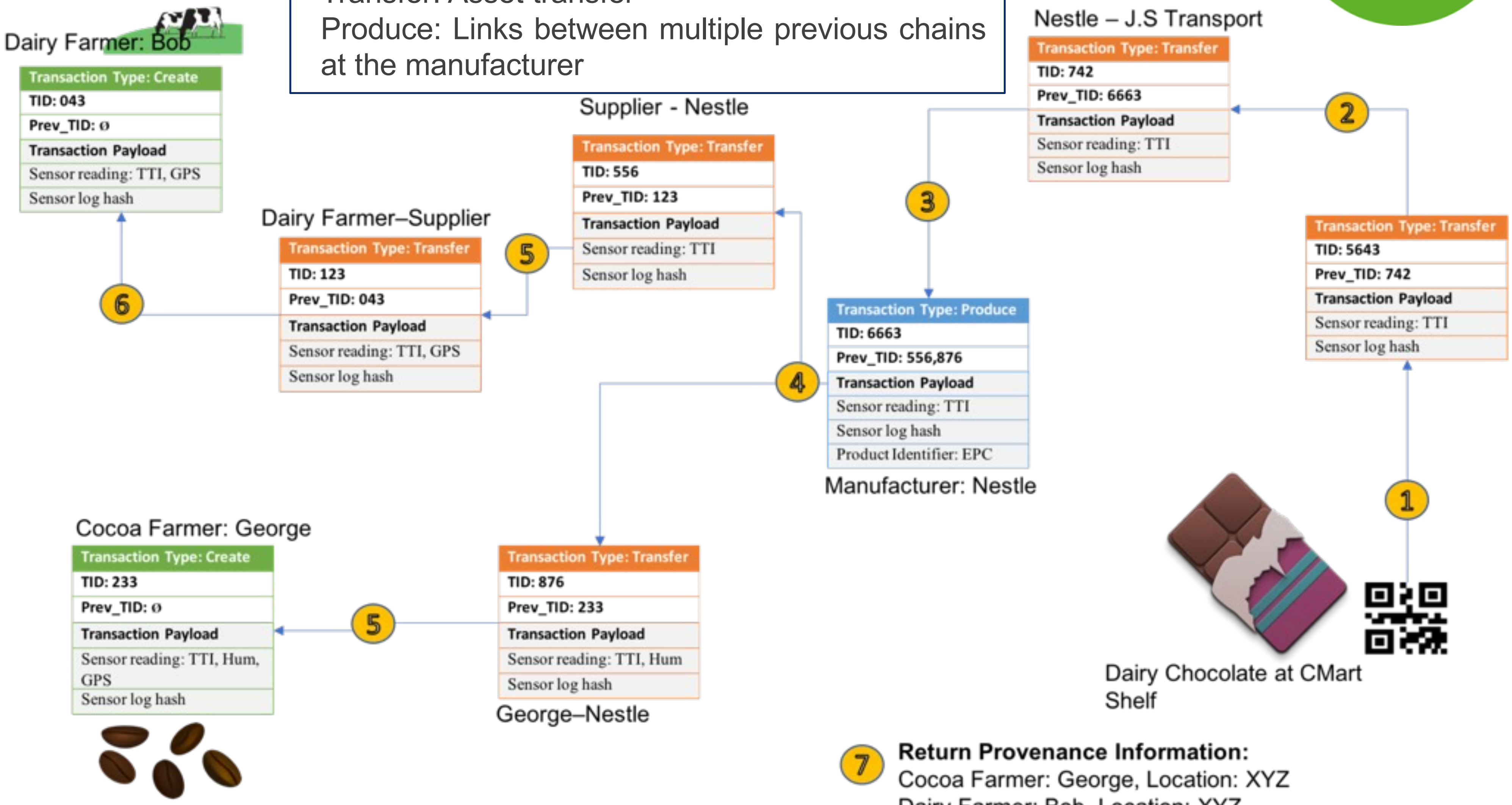
Geographical Sharding

Simplified Consensus



Transaction Flow from Farm to Fork

Create: Commodity existence
Transfer: Asset transfer
Produce: Links between multiple previous chains at the manufacturer



Dairy Farmer: Bob

Transaction Type: Create
TID: 043
Prev_TID: ø
Transaction Payload
Sensor reading: TTI, GPS
Sensor log hash

Dairy Farmer–Supplier

Transaction Type: Transfer
TID: 123
Prev_TID: 043
Transaction Payload
Sensor reading: TTI, GPS
Sensor log hash

Supplier - Nestle

Transaction Type: Transfer
TID: 556
Prev_TID: 123
Transaction Payload
Sensor reading: TTI
Sensor log hash

Nestle – J.S Transport

Transaction Type: Transfer
TID: 742
Prev_TID: 6663
Transaction Payload
Sensor reading: TTI
Sensor log hash

Transaction Type: Transfer
TID: 5643
Prev_TID: 742
Transaction Payload
Sensor reading: TTI
Sensor log hash

Transaction Type: Produce
TID: 6663
Prev_TID: 556,876
Transaction Payload
Sensor reading: TTI
Sensor log hash
Product Identifier: EPC

Manufacturer: Nestle

Cocoa Farmer: George

Transaction Type: Create
TID: 233
Prev_TID: ø
Transaction Payload
Sensor reading: TTI, Hum, GPS
Sensor log hash

Transaction Type: Transfer
TID: 876
Prev_TID: 233
Transaction Payload
Sensor reading: TTI, Hum
Sensor log hash

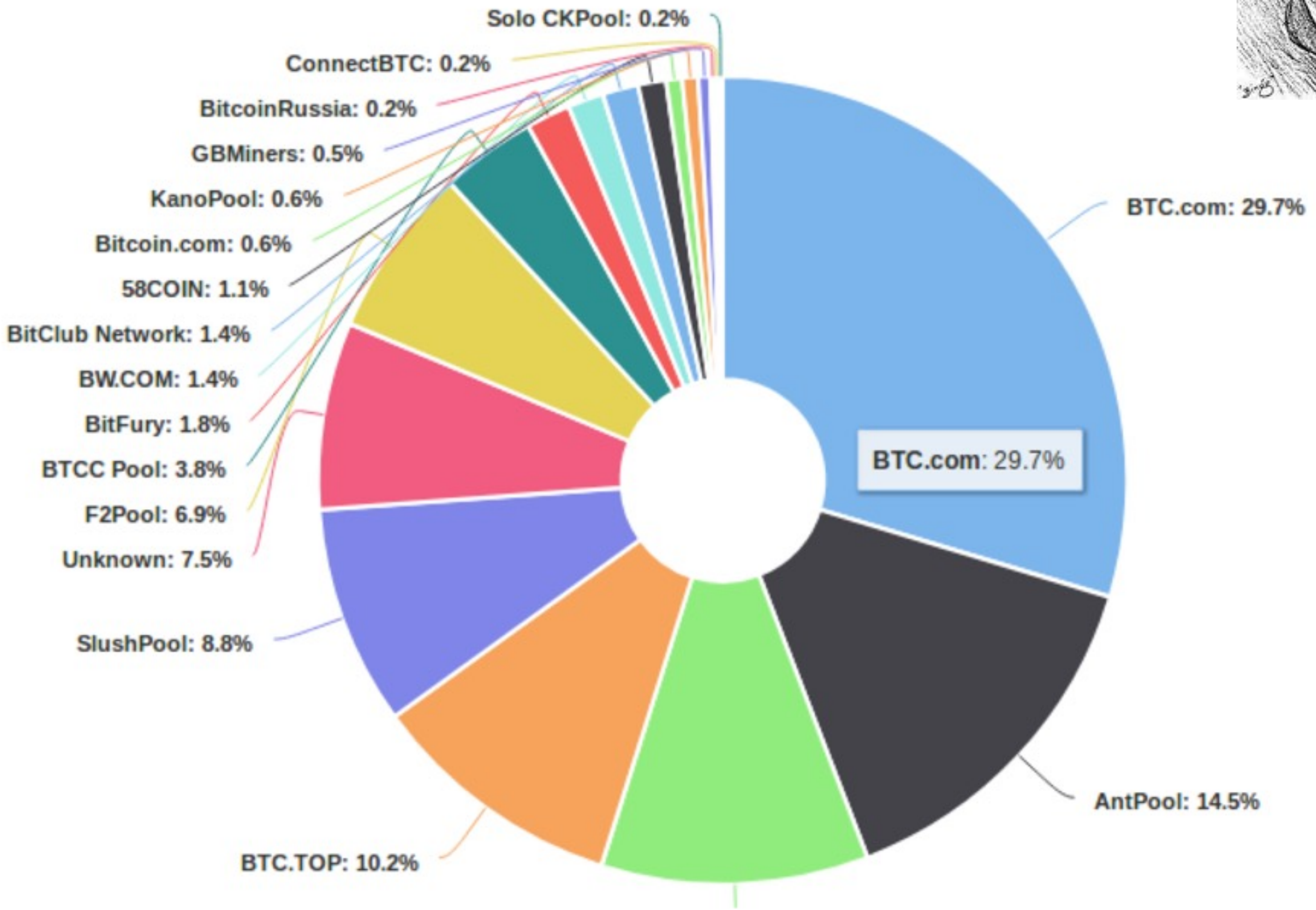
George–Nestle

Dairy Chocolate at CMart Shelf

7 **Return Provenance Information:**
Cocoa Farmer: George, Location: XYZ
Dairy Farmer: Bob, Location: XYZ

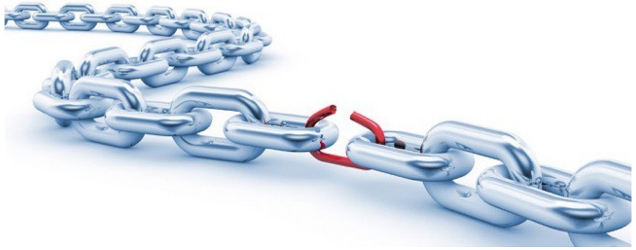
WE'VE GOT ISSUES

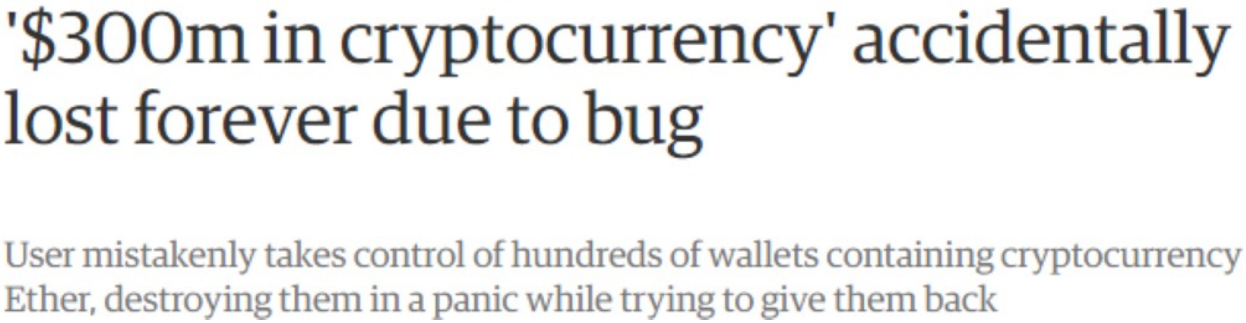
Centralisation of Power



There is a tendency to bigger pool sizes to reduce variance of earnings from mining.. this could be viewed as a failure of the protocol

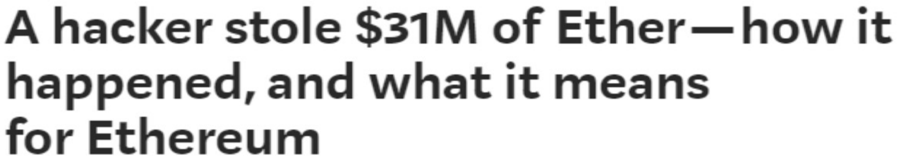
Blockchain Vulnerabilities



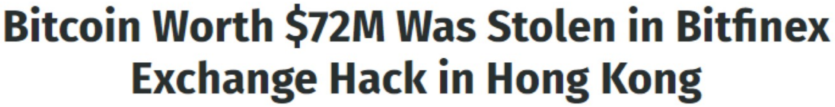


'$300m in cryptocurrency' accidentally lost forever due to bug

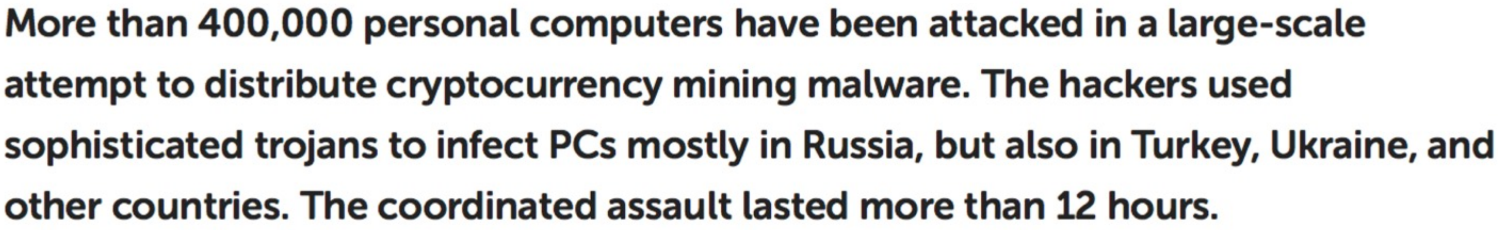
User mistakenly takes control of hundreds of wallets containing cryptocurrency Ether, destroying them in a panic while trying to give them back



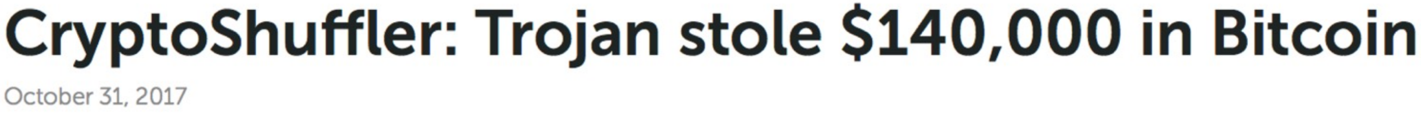
A hacker stole $31M of Ether — how it happened, and what it means for Ethereum



Bitcoin Worth $72M Was Stolen in Bitfinex Exchange Hack in Hong Kong

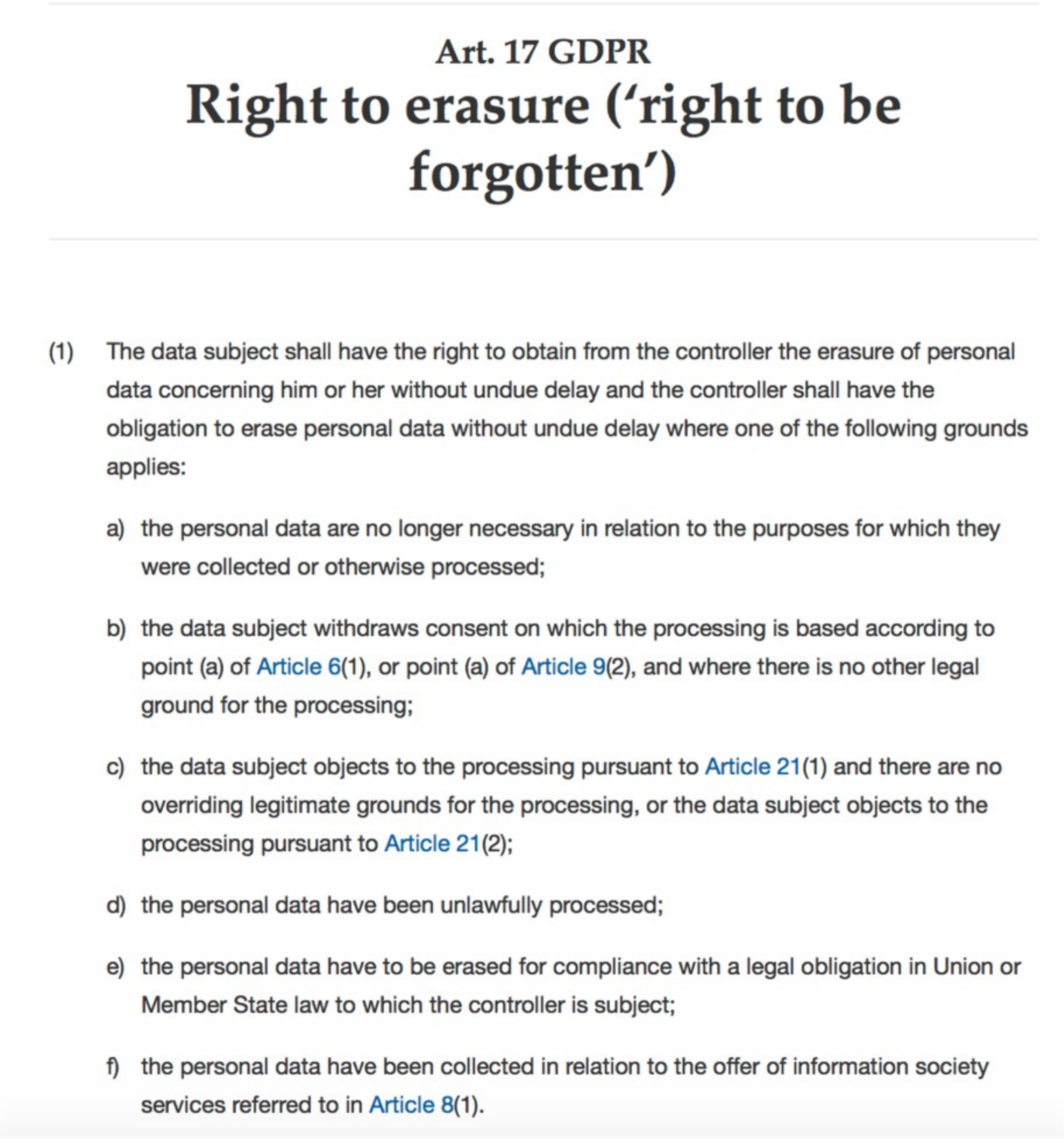


More than 400,000 personal computers have been attacked in a large-scale attempt to distribute cryptocurrency mining malware. The hackers used sophisticated trojans to infect PCs mostly in Russia, but also in Turkey, Ukraine, and other countries. The coordinated assault lasted more than 12 hours.



CryptoShuffler: Trojan stole $140,000 in Bitcoin

October 31, 2017



Art. 17 GDPR

Right to erasure ('right to be forgotten')

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

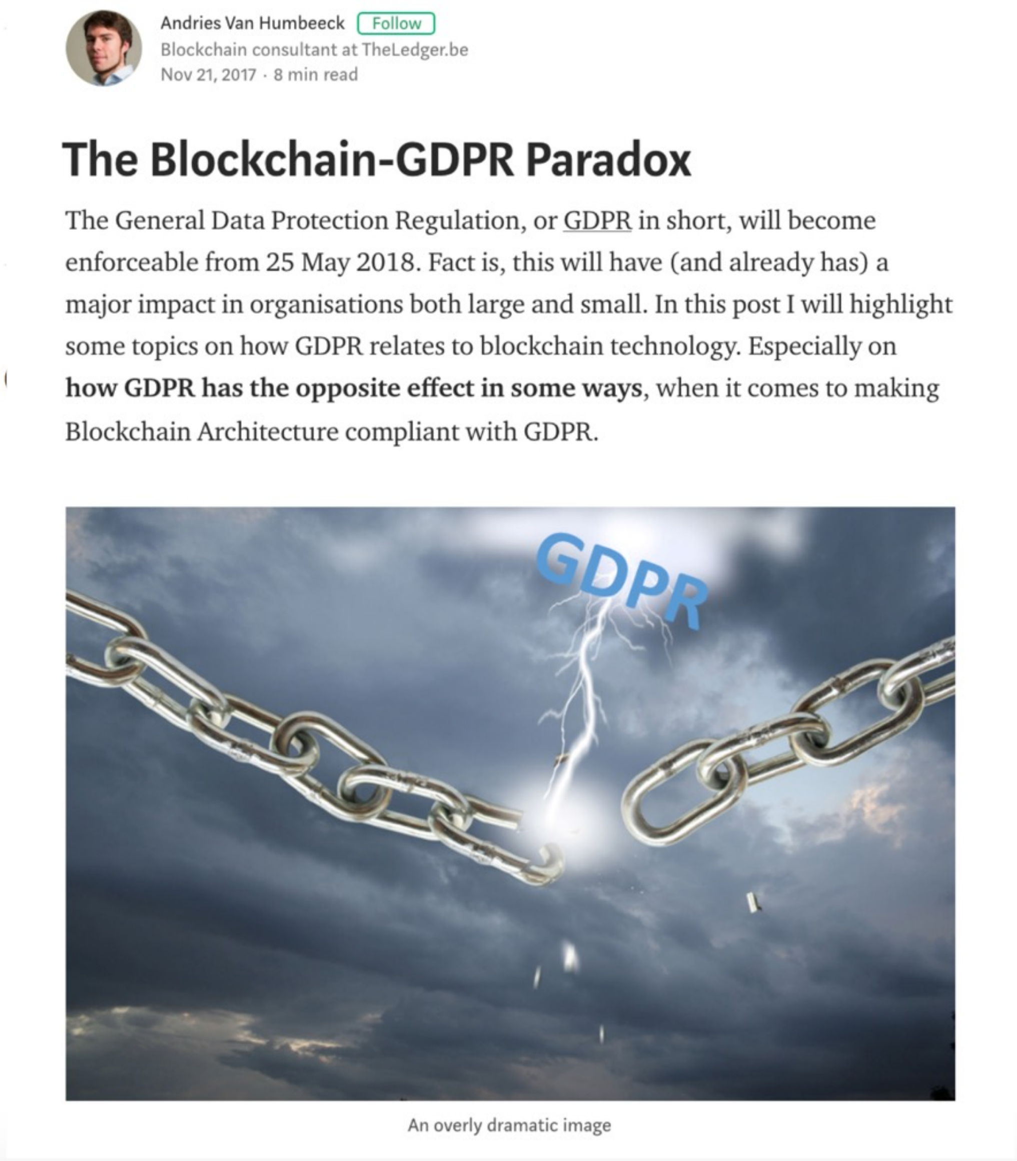
c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

d) the personal data have been unlawfully processed;

e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

KEEP
CALM
AND
COMPLY WITH
GDPR



Andries Van Humbeeck Follow
Blockchain consultant at TheLedger.be
Nov 21, 2017 · 8 min read

The Blockchain-GDPR Paradox

The General Data Protection Regulation, or GDPR in short, will become enforceable from 25 May 2018. Fact is, this will have (and already has) a major impact in organisations both large and small. In this post I will highlight some topics on how GDPR relates to blockchain technology. Especially on **how GDPR has the opposite effect in some ways**, when it comes to making Blockchain Architecture compliant with GDPR.

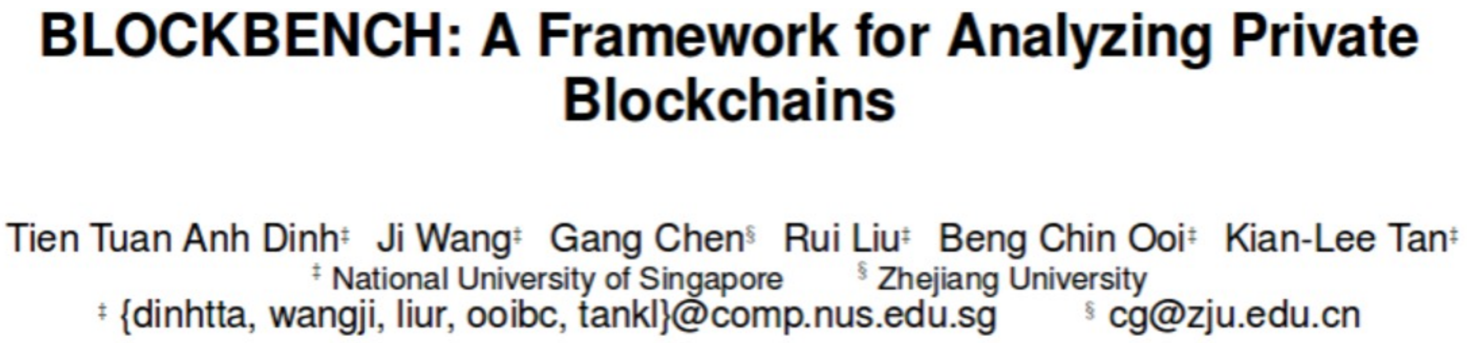
An overly dramatic image

Memory Optimized & Flexible Blockchain (MOF-BC)

- Enables participants to remove or summarize their transactions and age their data and to exercise the "right to be forgotten”
- User-Initiated (UIMO) or SP-Initiated Memory Optimization (SIMO)
- Option to offload optimization to the network (NIMO)
- Memory Optimization Modes (MoMs)
  - Temporary
  - Summarizable
  - Permanent
- Modification to the way the block hash is computed
- Batch removals for optimizing overheads associated with removal of transactions
- Rewards offered to nodes for employing optimization

A. Dorri, S. S. Kanhere, R. Jurdak, MOF-BC: A Memory Optimized and Flexible BlockChain for Large Scale Networks (under review), https://arxiv.org/abs/1801.04416

What about performance?



BLOCKBENCH: A Framework for Analyzing Private Blockchains

Tien Tuan Anh Dinh[‡] Ji Wang[‡] Gang Chen[§] Rui Liu[‡] Beng Chin Ooi[‡] Kian-Lee Tan[‡]
[‡] National University of Singapore [§] Zhejiang University
[‡] {dinhtta, wangji, liur, ooibc, tankl}@comp.nus.edu.sg [§] cg@zju.edu.cn

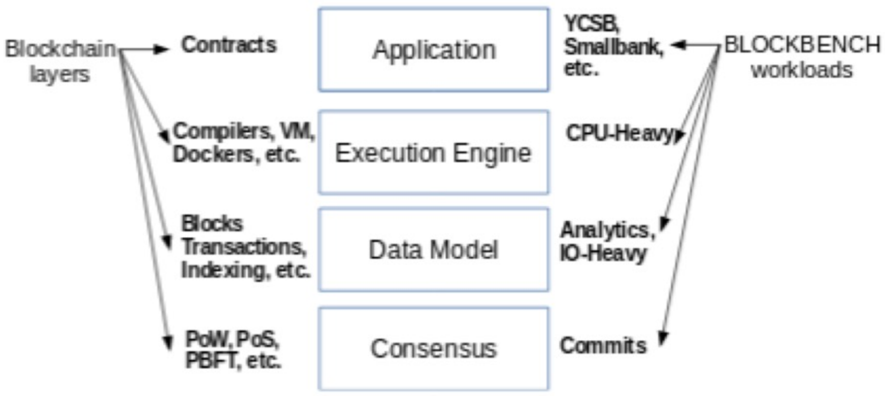
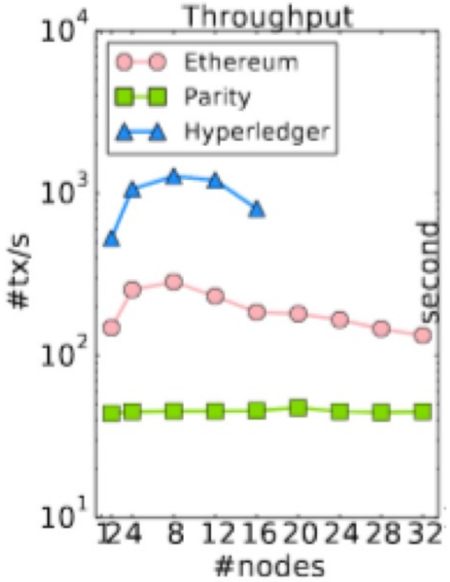
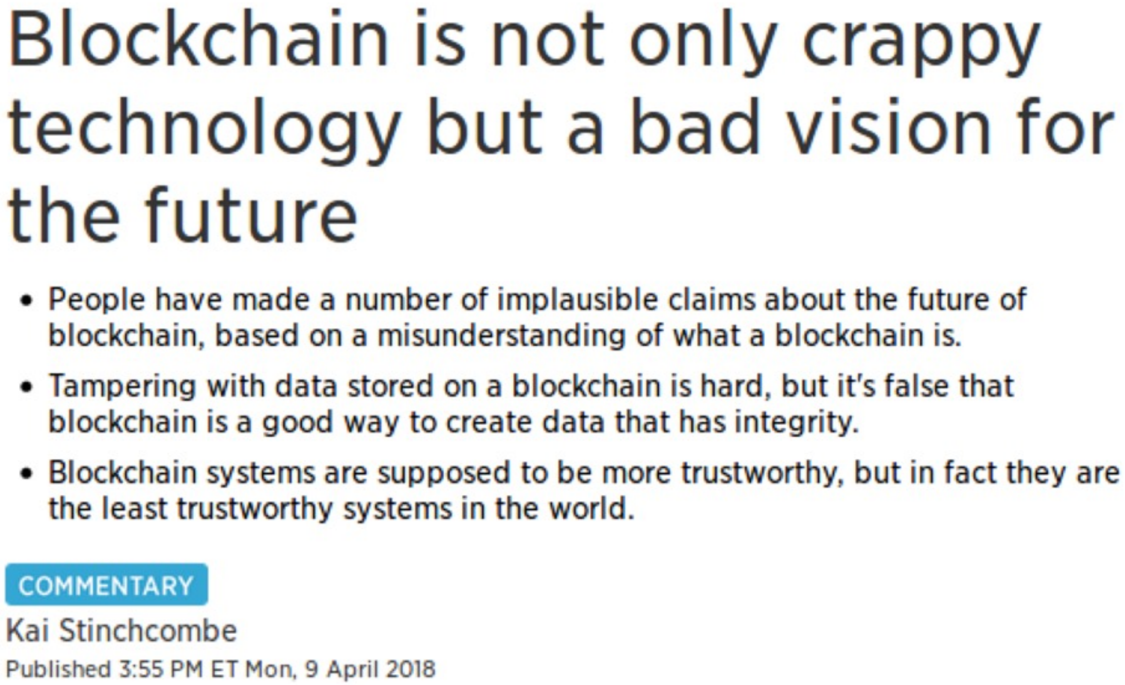


Figure 3: Abstraction layers in blockchain, and the corresponding workloads in BLOCKBENCH.



https://arxiv.org/pdf/1703.04057.pdf

Trust?



Blockchain is not only crappy technology but a bad vision for the future

- People have made a number of implausible claims about the future of blockchain, based on a misunderstanding of what a blockchain is.
- Tampering with data stored on a blockchain is hard, but it's false that blockchain is a good way to create data that has integrity.
- Blockchain systems are supposed to be more trustworthy, but in fact they are the least trustworthy systems in the world.

COMMENTARY

Kai Stinchcombe

Published 3:55 PM ET Mon, 9 April 2018

Source: CNBC

"A person who sprayed pesticides on a mango can still enter onto a blockchain system that the mangoes were organic.”

“Projects based on the elimination of trust have failed to capture customers' interest *because trust is actually so damn valuable*. A lawless and mistrustful world where self-interest is the only principle and paranoia is the only source of safety is a not a paradise but a crypto-medieval hellhole.”

“As a society, and as technologists and entrepreneurs in particular, we're going to have to get good at cooperating—at building trust, and, at being trustworthy. Instead of directing resources to the *elimination* of trust, we should direct our resources to the *creation* of trust—whether we use a long series of sequentially hashed files as our storage medium or not.”

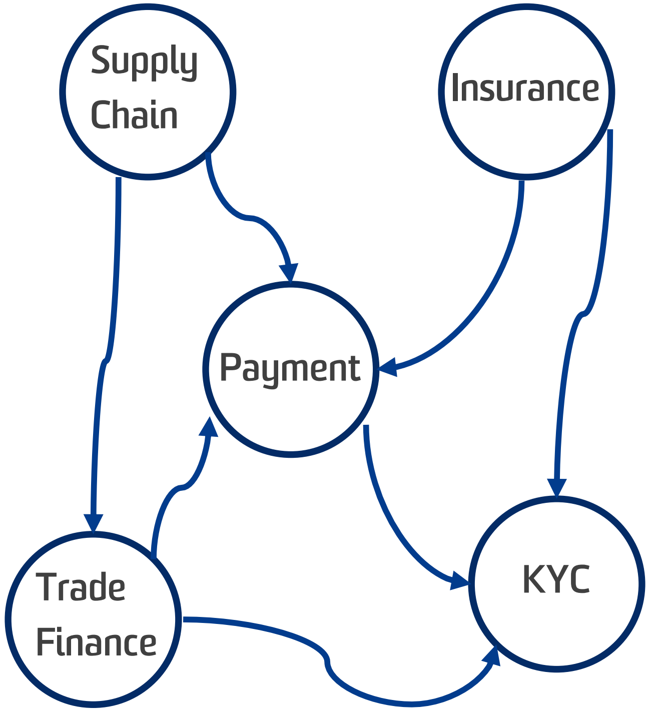
Privacy

- Particularly an issue with public blockchains

- Cryptographically secure obfuscation (holy grail) is difficult

- Possible Approaches:
  - Secure Multi-party Computation
  - Zero Knowledge Proofs (SNARKs in particular)

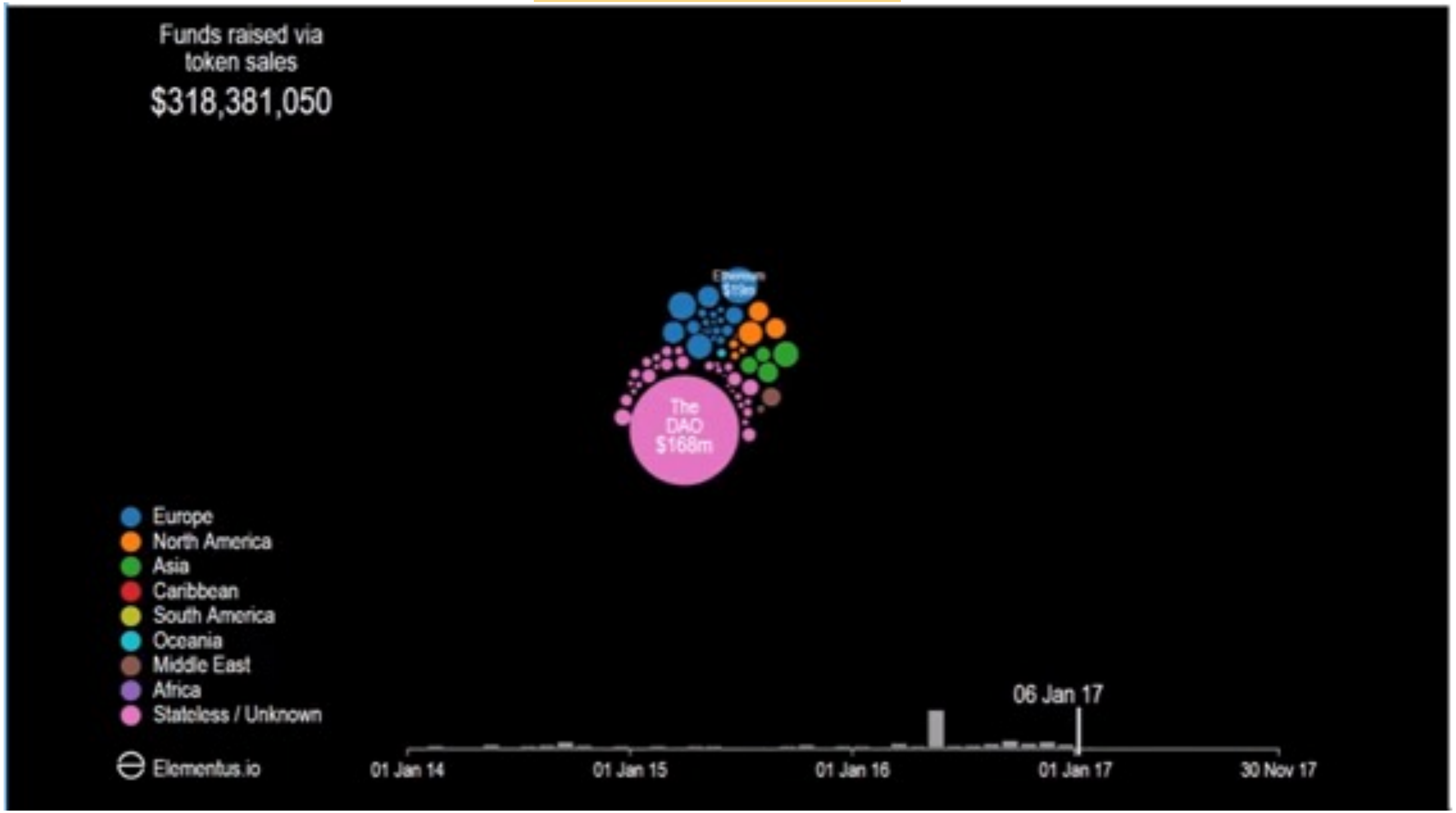
Internet of Blockchains



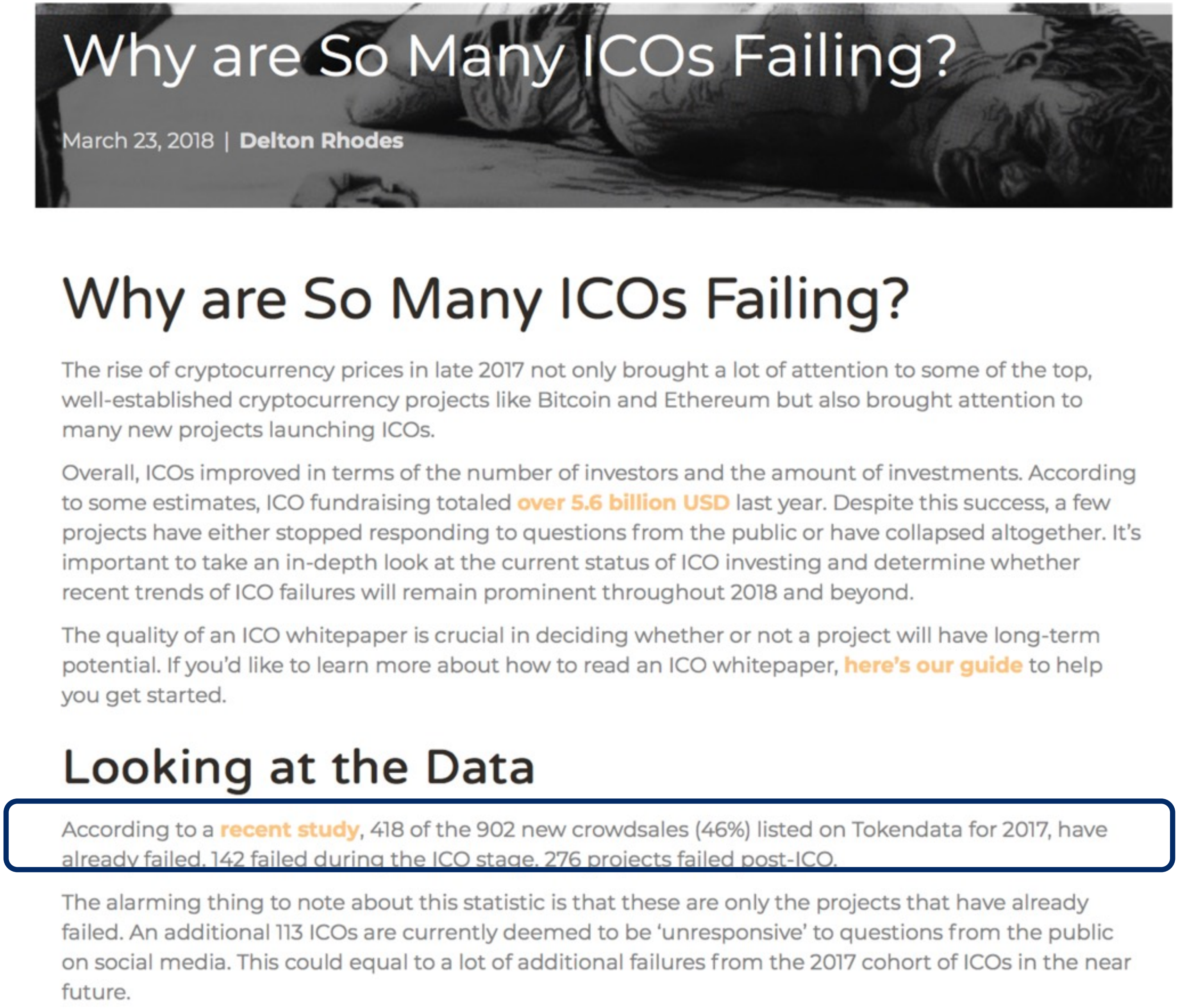
Cross-industry and cross-chain interoperability for broader application scenarios

Interledger Protocol (ILP): Open standard for interledger token exchange

Cosmos: multiple disparate blockchains (zones) with a central hub for coordination



Source: Elementus.io



Why are So Many ICOs Failing?

March 23, 2018 | **Delton Rhodes**

Why are So Many ICOs Failing?

The rise of cryptocurrency prices in late 2017 not only brought a lot of attention to some of the top, well-established cryptocurrency projects like Bitcoin and Ethereum but also brought attention to many new projects launching ICOs.

Overall, ICOs improved in terms of the number of investors and the amount of investments. According to some estimates, ICO fundraising totaled **over 5.6 billion USD** last year. Despite this success, a few projects have either stopped responding to questions from the public or have collapsed altogether. It's important to take an in-depth look at the current status of ICO investing and determine whether recent trends of ICO failures will remain prominent throughout 2018 and beyond.

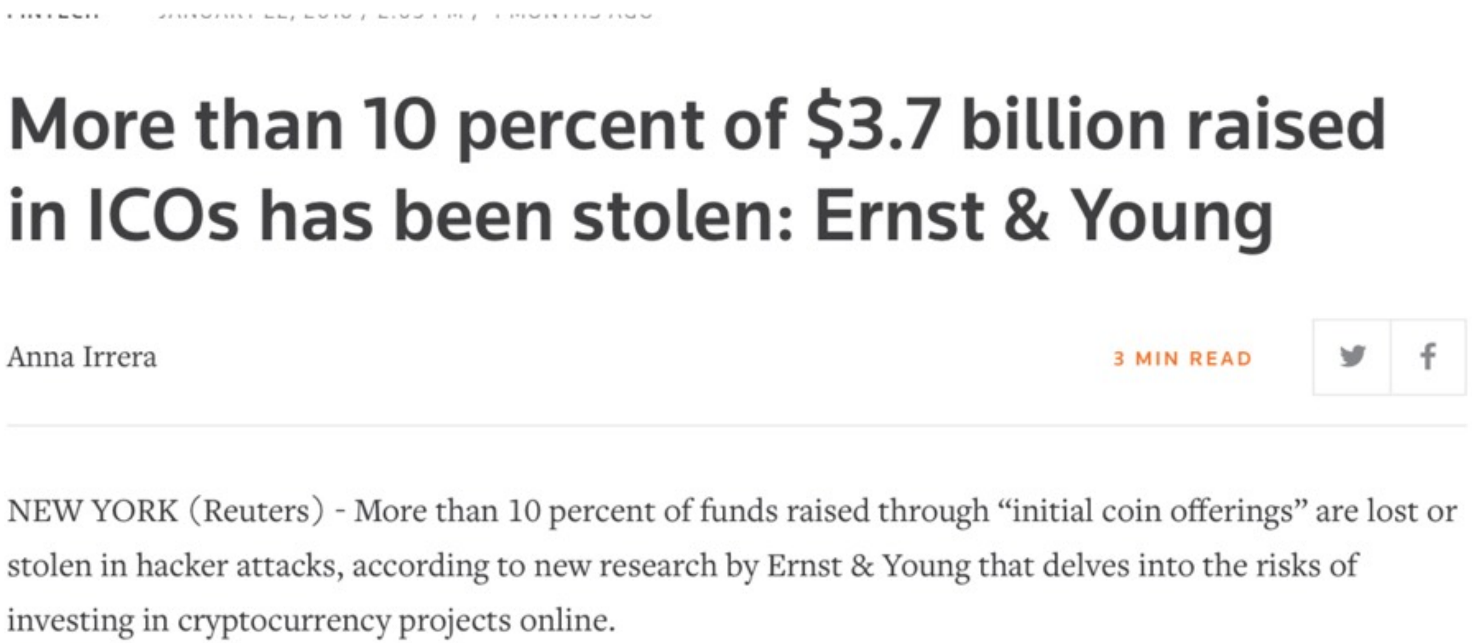
The quality of an ICO whitepaper is crucial in deciding whether or not a project will have long-term potential. If you'd like to learn more about how to read an ICO whitepaper, **here's our guide** to help you get started.

Looking at the Data

According to a **recent study**, 418 of the 902 new crowdsales (46%) listed on Tokendata for 2017, have already failed. 142 failed during the ICO stage. 276 projects failed post-ICO.

The alarming thing to note about this statistic is that these are only the projects that have already failed. An additional 113 ICOs are currently deemed to be 'unresponsive' to questions from the public on social media. This could equal to a lot of additional failures from the 2017 cohort of ICOs in the near future.

Source: www.coincentral.com



More than 10 percent of $3.7 billion raised in ICOs has been stolen: Ernst & Young

Anna Irrera

NEW YORK (Reuters) - More than 10 percent of funds raised through “initial coin offerings” are lost or stolen in hacker attacks, according to new research by Ernst & Young that delves into the risks of investing in cryptocurrency projects online.

Source: Wired

Source: zdnet

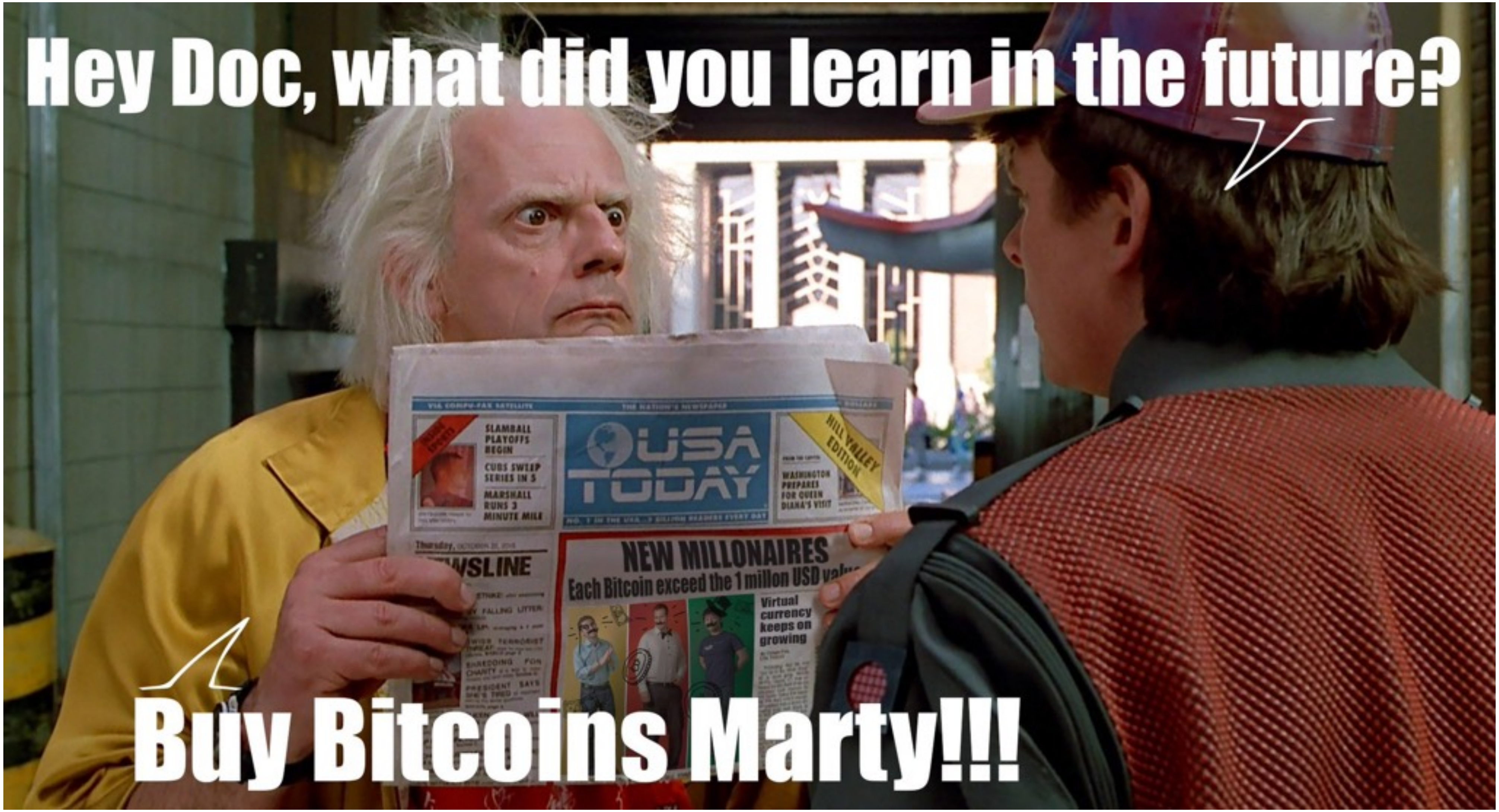
Conclusions

Still early days, but potential for blockchain technologies for next-generation decentralized networks and applications is clear

Many interesting directions:

- Mathematical modeling of blockchains
- Ways to improve scalability and performance
- New architectures
- New applications
- Smart(er) contracts with machine learning?

Research opportunities pertaining to security, distributed systems, networks, software engineering, databases, cloud computing, financial engineering, network economics, Internet of things,…


Hey Doc, what did you learn in the future?
Buy Bitcoins Marty!!!
USA TODAY
SLAMBALL PLAYOFFS BEGIN
CUBS SWEEP SERIES IN 5
MARSHALL RUNS 3 MINUTE MILE
HILL VALLEY EDITION
WASHINGTON PREPARES FOR QUEEN DIANA'S VISIT
WSLINE
NEW MILLONAIRES
Each Bitcoin exceed the 1 millon USD val
Virtual currency keeps on growing

W: www.salilkanhere.net, E: salil.kanhere@unsw.edu.au