



Blockchain for Cyberphysical Systems: Applications, Opportunities and Challenges



Prof. Salil Kanhere, Ali Dorri

School of Computer Science and Engineering
UNSW Sydney

Australia

E: {salil.kanhere, ali.dorri}@unsw.edu.au

W: www.salilkanhere.net

Prof. Raja Jurdak

Distributed Sensing Systems Group

Data61 CSIRO, Brisbane

Australia

E: raja.jurdak@data61.csiro.au

W: www.jurdak.com

W: <https://research.csiro.au/dss/>

All Articles Referenced can be accessed at - <https://tinyurl.com/icbc2019>

Acknowledgements

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

Data61 CSIRO: Volkan Dedeogulu

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



University of Zurich: Burkhard Stiller



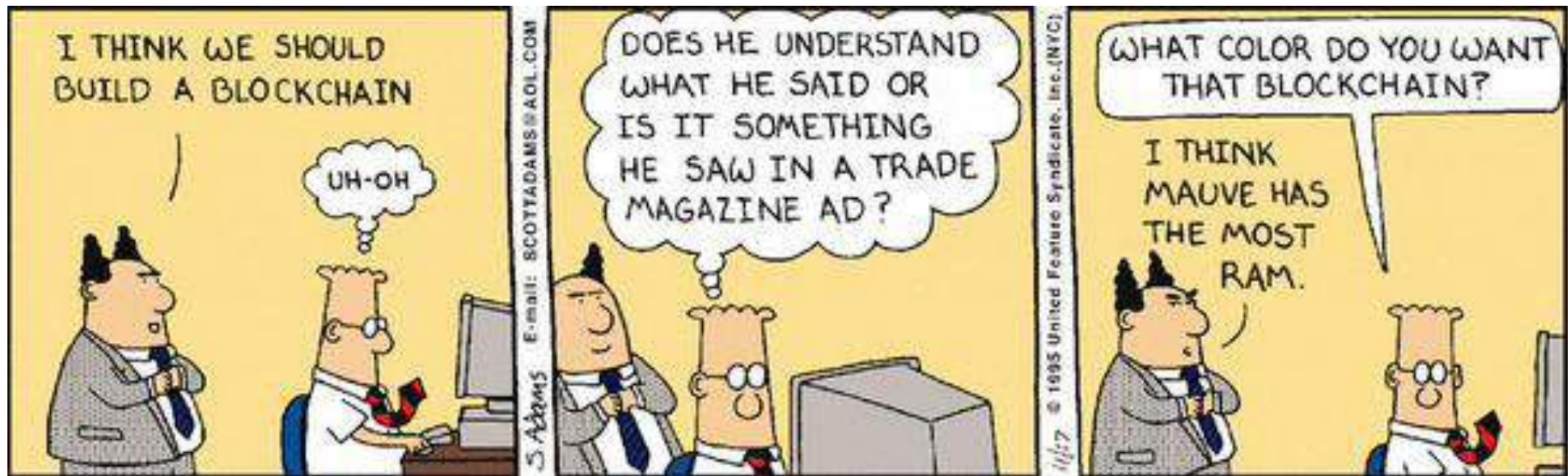
**Universität
Zürich** ^{UZH}

University of Sydney: Fengjie Luo

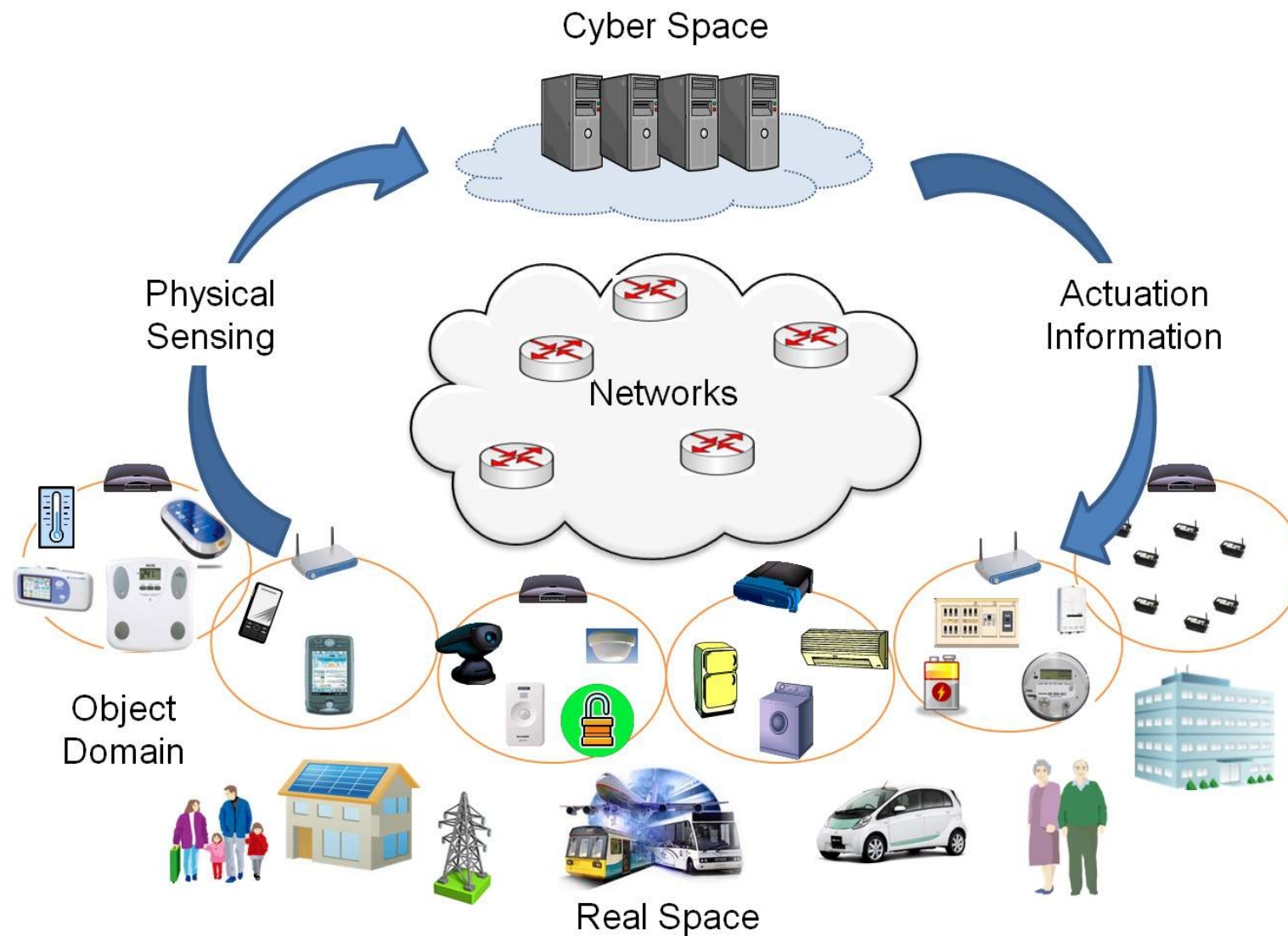


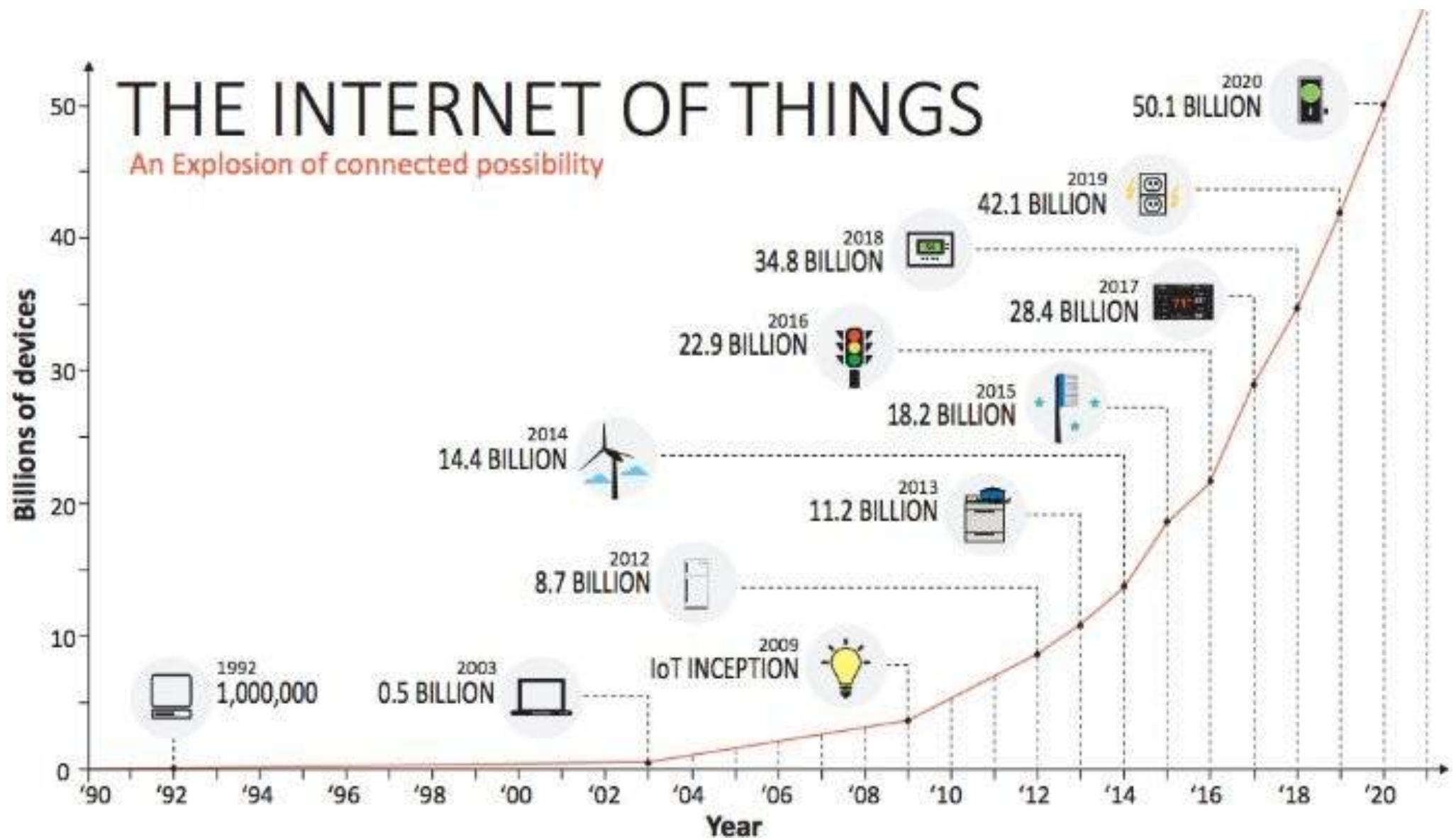
Tutorial Outline

- Introduction (Raja)
- Blockchain and the Internet of Things (Raja)
- Blockchain in Supply Chains (Salil)
- Blockchain in Connected Vehicles (Salil)
- Blockchain in Energy Trading (Ali)
- Open Issues, Conclusions (Ali)



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





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



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



1

Internet of Things



Motivating Example



Motivating Example



Challenges of adopting blockchain in IoT



- Complex Consensus Algorithms
- Scale and associated overheads
- Latency
- Throughput
- Complex security mechanisms (e.g. for preventing double spending) may not be relevant
- Incentives

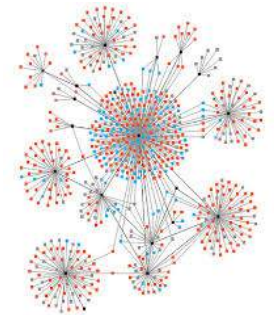


Lightweight Scalable Blockchain (LSB) for IoT



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



A. Dorri, S. Kanhere, R. Jurdak., and P. Gauravaram, “Blockchain for IoT Security and Privacy: The Case Study of a Smart Home,” Workshop on security, privacy, and trust in the Internet of things (PERCOM), March, 2017.

A. Dorri, S. S. Kanhere, and R. Jurdak, “Towards an Optimized BlockChain for IoT”, (IoT DI) 2017

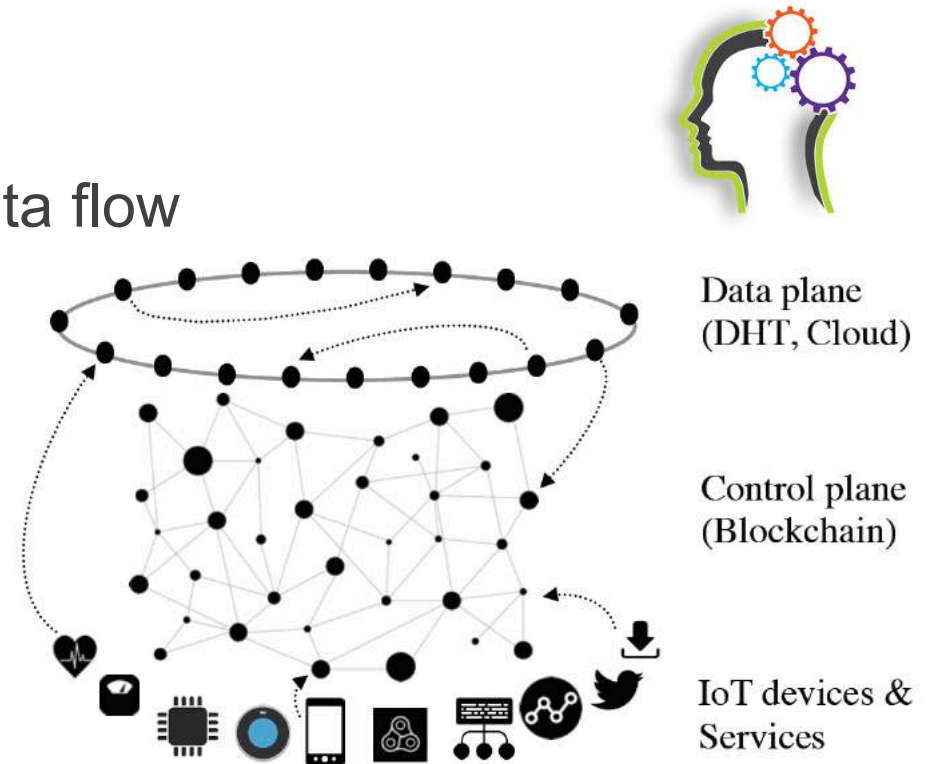
A. Dorri, S. S. Kanhere, R. Jurdak and Praveen Gauravaram, “A Lightweight Scalable Blockchain for IoT Security and Privacy”, under review, <https://arxiv.org/abs/1712.02969>

Some fundamental concepts

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

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

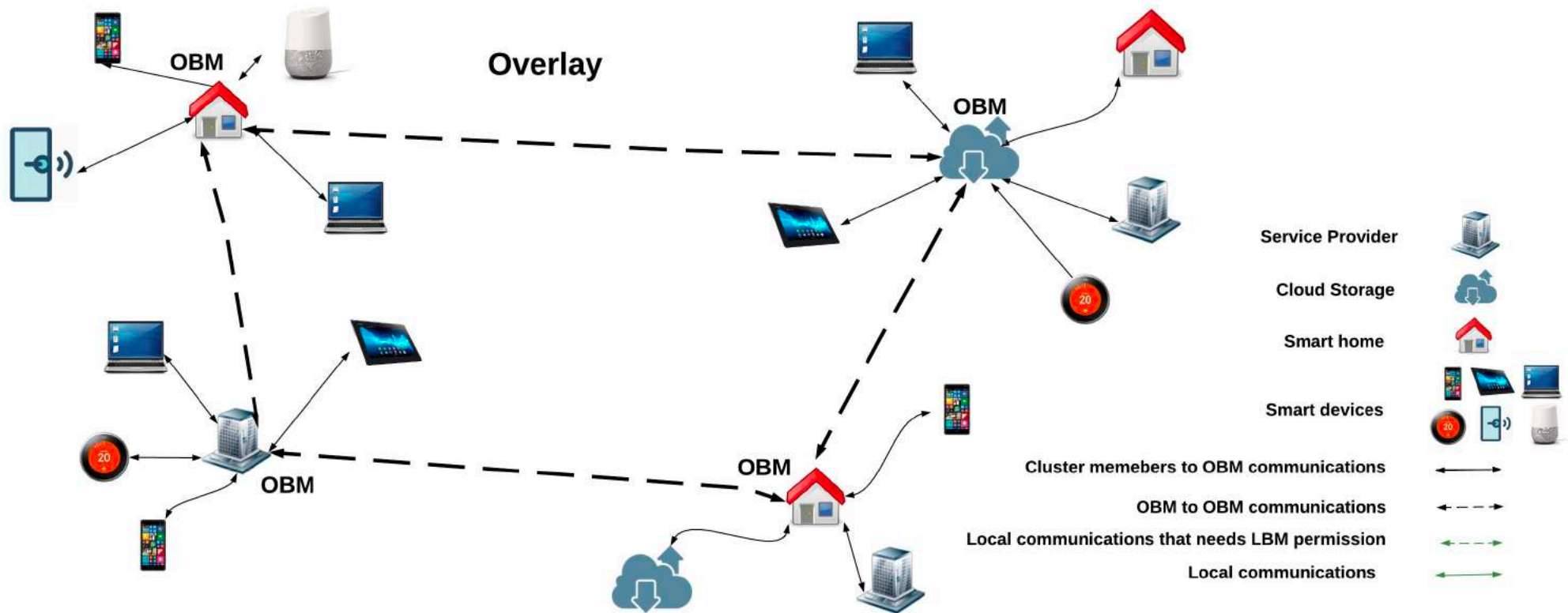
- Cloud storage
- Local storage (where relevant)



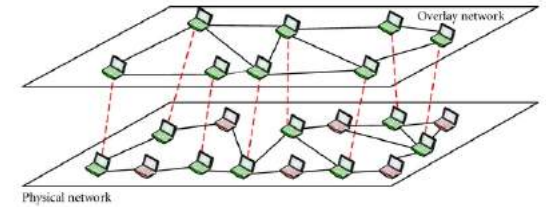
Overlay Block Manager (OBM): Entity responsible for managing the blockchain

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

LSB Overview



Overlay



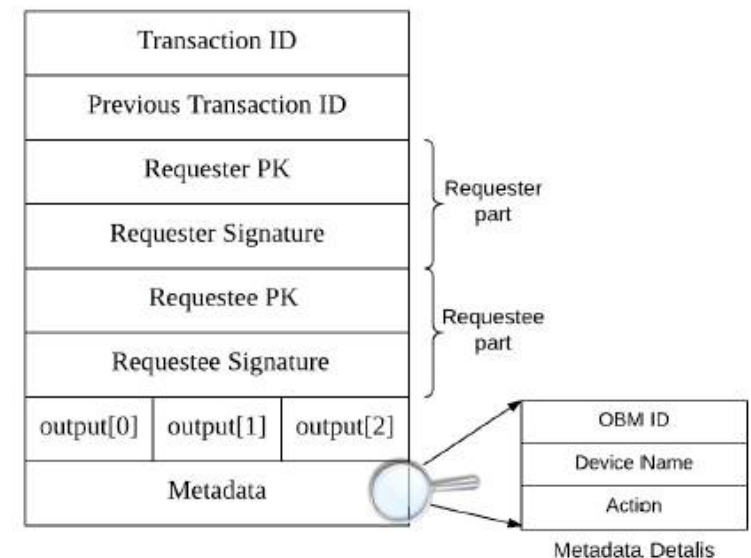
Each node is known by a public key (changeable for anonymity)

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

Transactions are digitally signed using 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.

OBTMs 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



Distributed 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

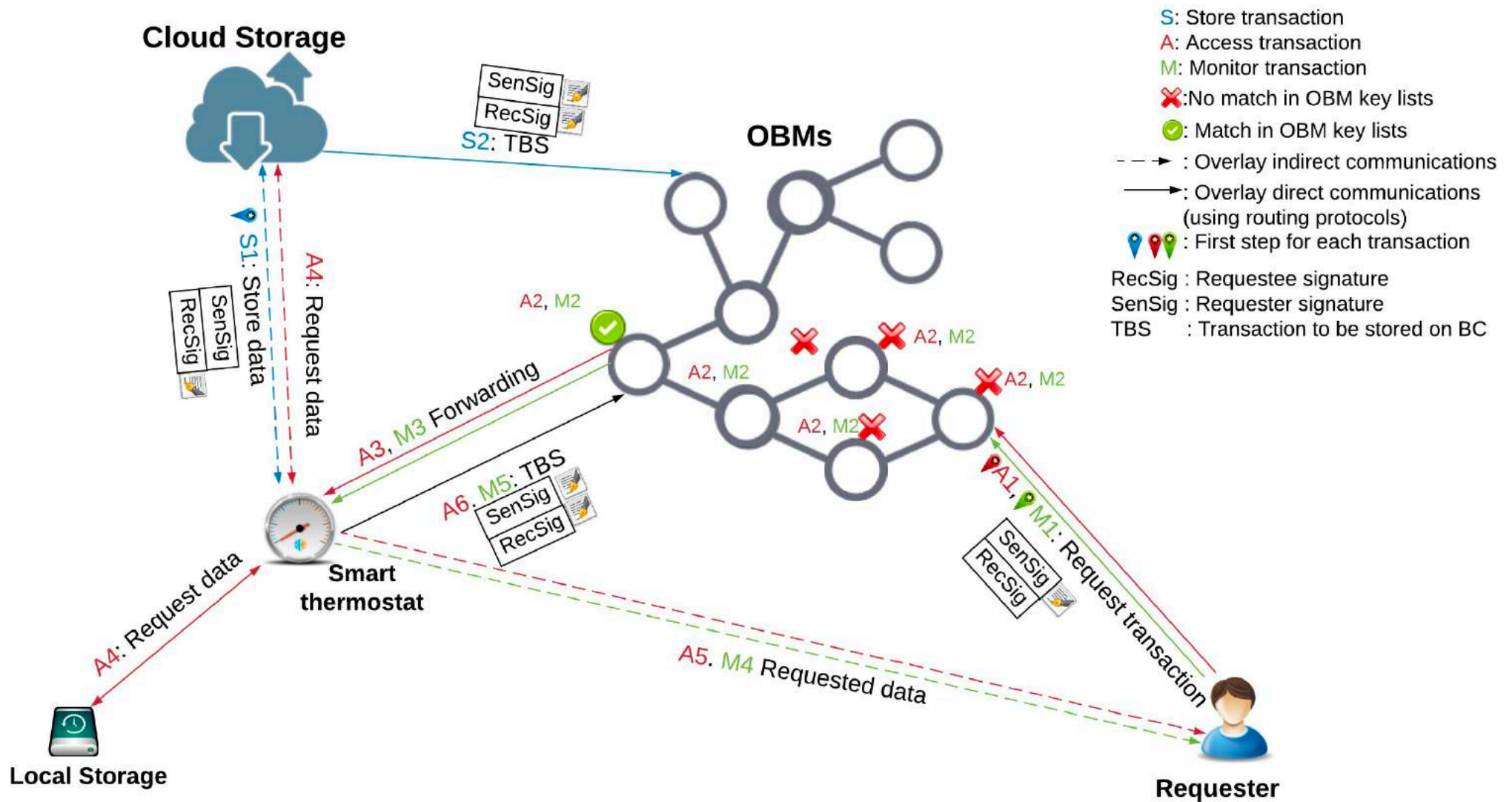
Goal : $\alpha_{\min} \leq \alpha \leq \alpha_{\max}$

$$\alpha = \frac{N * R * \text{Consensus-period}}{T_{\max} * M}$$

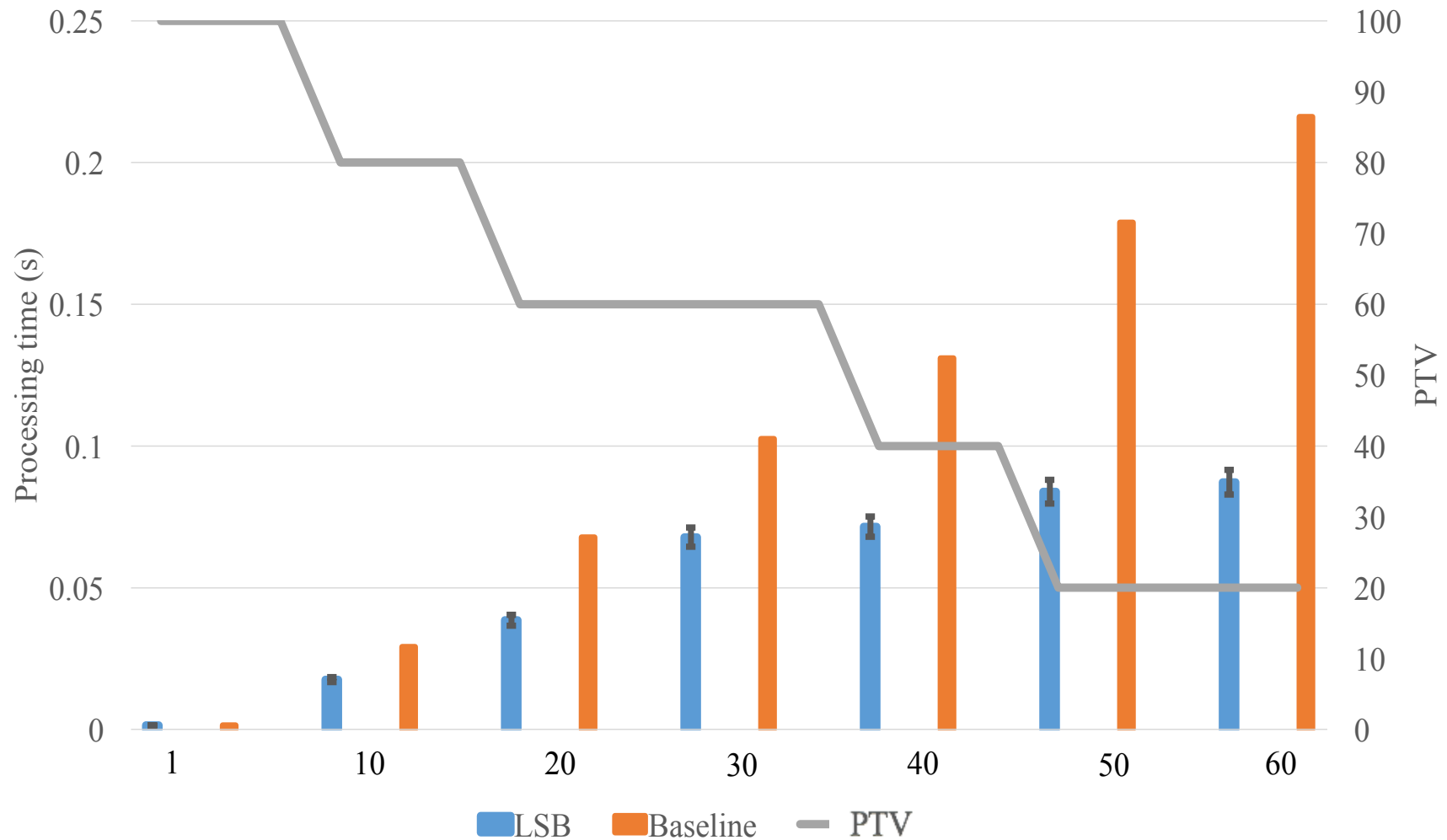
Tune two parameters to guarantee the above condition

- *Consensus-period*
- The number of OBM's (M)

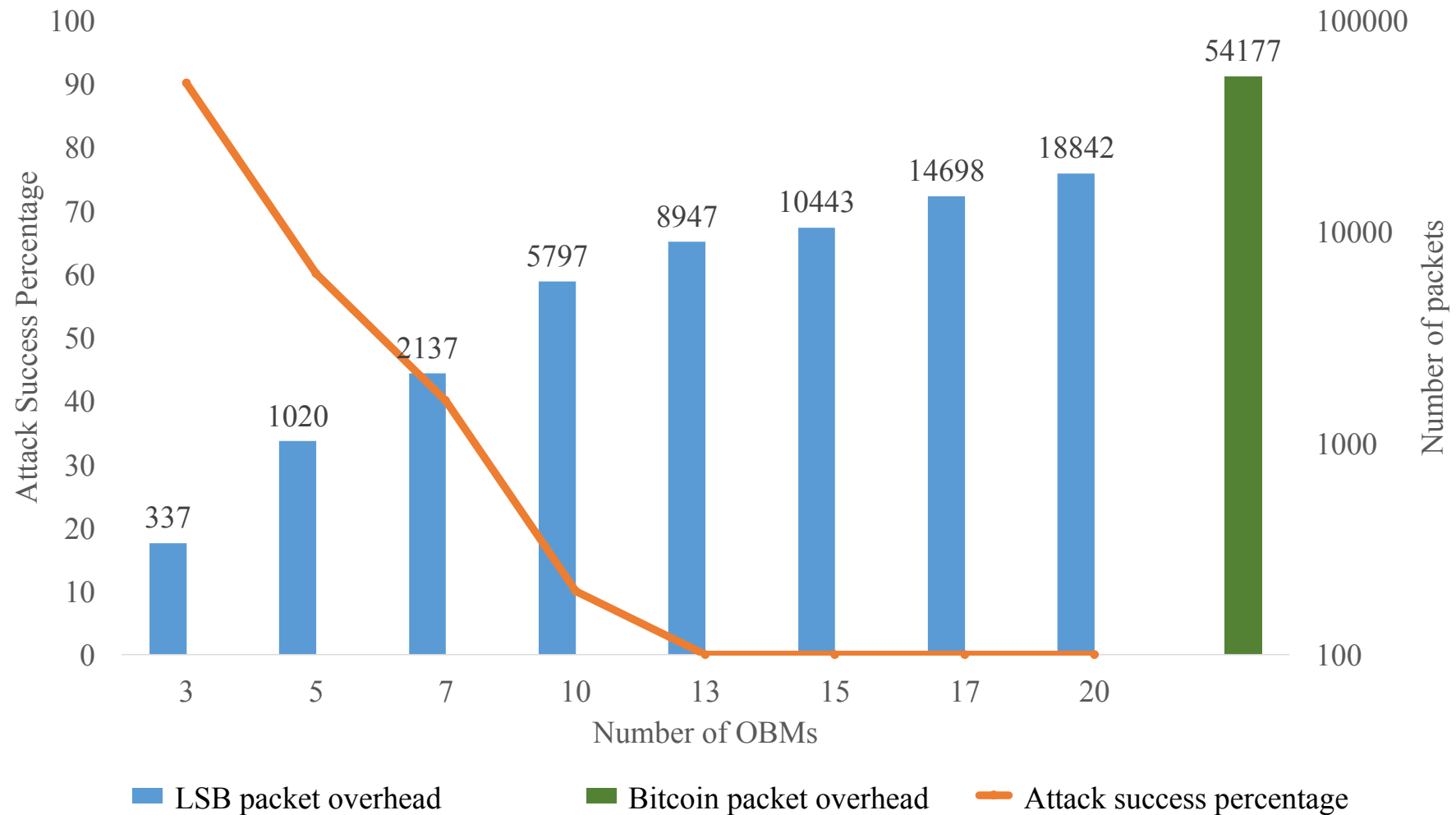
Transaction Flow



Distributed Trust

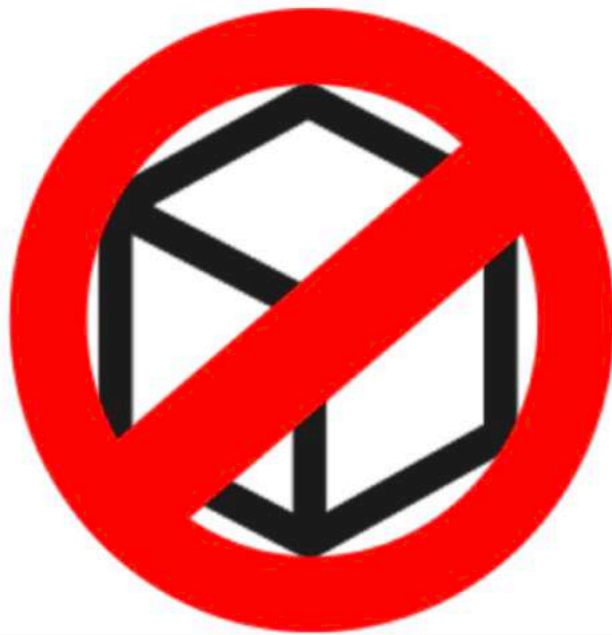


Resilience to Attacks

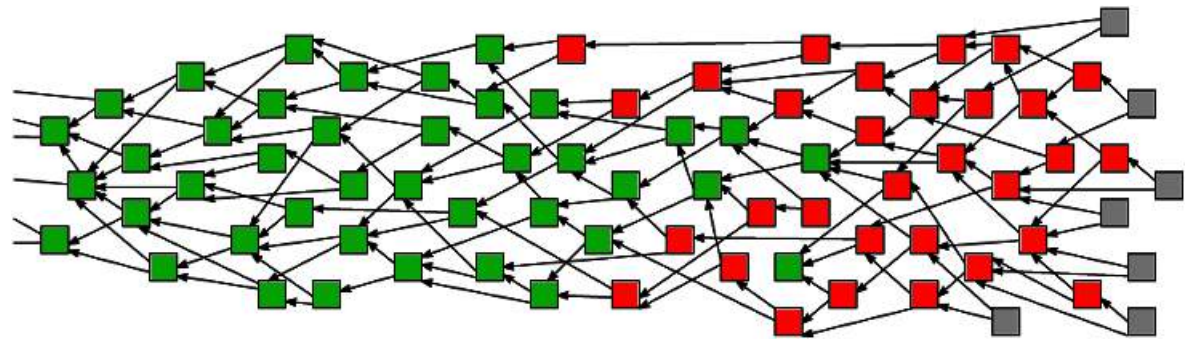




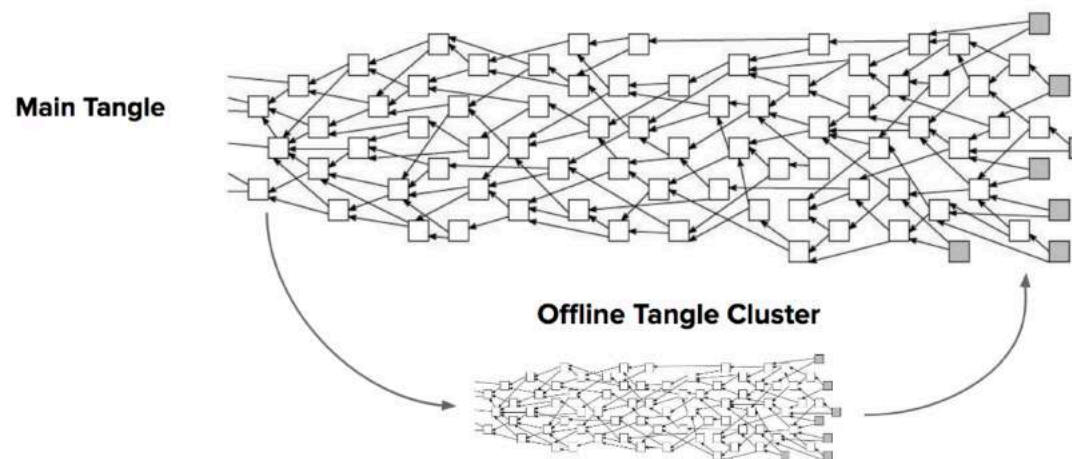
A Blockchain **without the Blocks** and the **Chain**

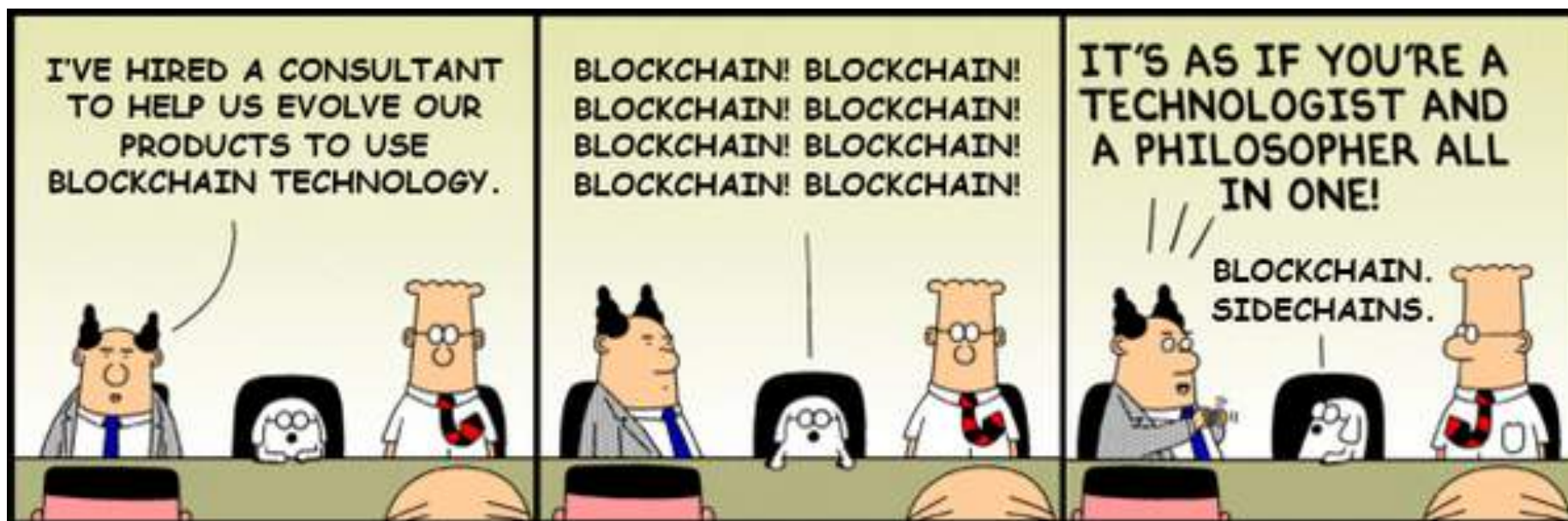


Tangle



- 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)





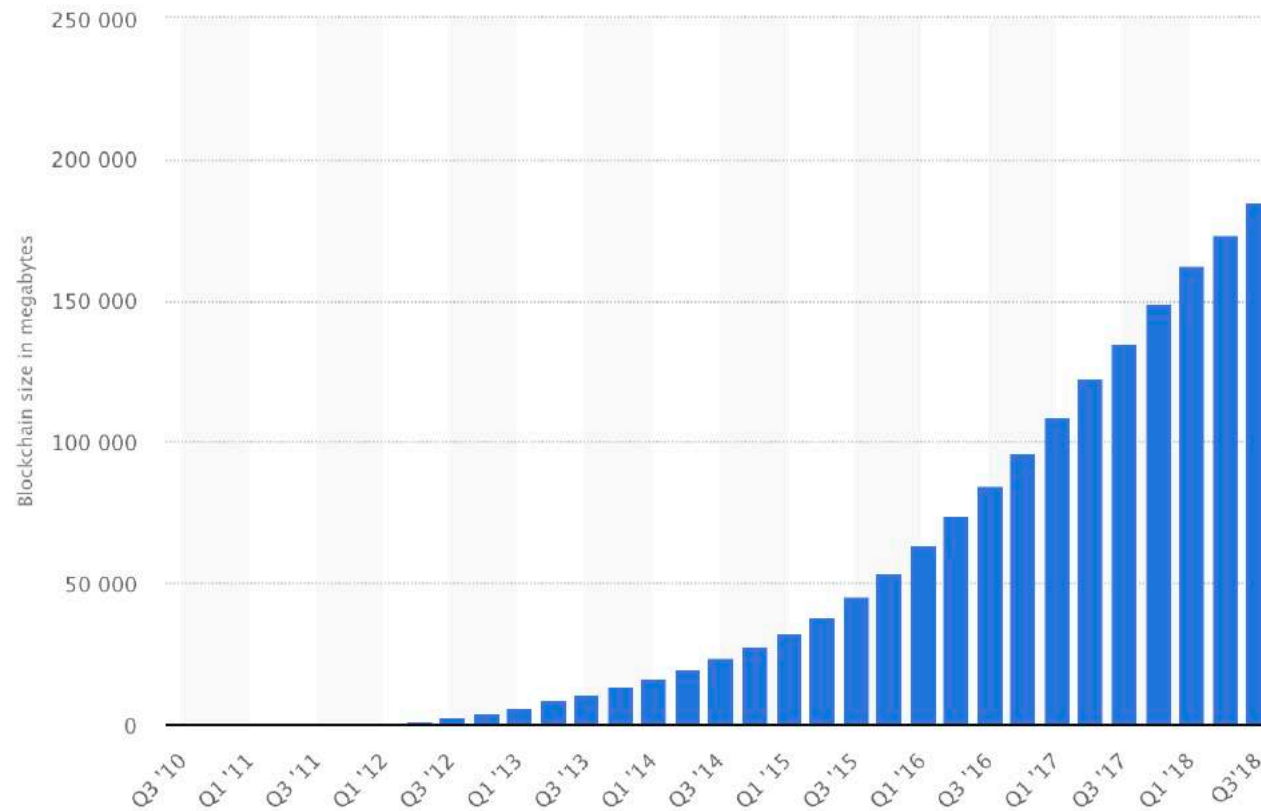
Immutability: The good ...

Blockchain immutability ensures

- **Security** as blockchain is tamper-resistant
- **Auditability** as all transaction are recorded permanently
- **Double spending protection** as the spent transaction cannot be denied (or removed)



...the bad...



Bitcoin blockchain size grows significantly

... the really bad...



Persistent data and privacy risks

- All transactions of an IoT user is stored in the blockchain
- The transactions contain the pattern of communications of IoT devices
- Attackers may deanonymize the user by classifying his transactions in blockchain
- If the key of a user is revealed, all the history of his actions as well as devices communications will be revealed



NEWS

BLOCKCHAIN TECH

GDPR Vs. Blockchain – Technology Against The Law

How Does 'The Right To Be Forgotten' Exist Alongside An Immutable Ledger?

... and the ugly

NEWS

SET LOCATION
for local news & weather

[Home](#) [Just In](#) [Politics](#) [World](#) [Business](#) [Sport](#) [Science](#) [Health](#) [Arts](#) [Analysis](#) [Fact Check](#) [More](#)

BREAKING NEWS Emergency services say several evacuation routes have been cut off by the Deepwater bushfires in central Queensland and that residents will have to be ferried across a creek by boat. [Read more...](#)

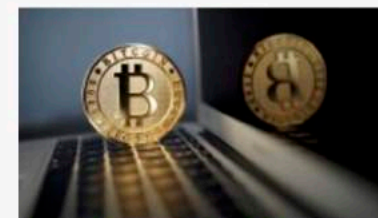
[Print](#) [Email](#) [Facebook](#) [Twitter](#) [More](#)

Bitcoin's blockchain contains child abuse images, meaning the cryptocurrency's possession could be 'illegal'

Updated 23 Jul 2018, 9:34pm



CRYPTOCURRENCIES



'Lust for wealth': Why we buy cryptocurrency despite the risks



Will those who've made cryptocurrency profits pay their tax?



Requirements for IoT Applications



- Blockchain transactions may be linked to data in cloud storage
- Diverse storage requirements in IoT applications
 - Temporary storing
 - Summarizing transactions
 - Aging data
 - Permanently storing

Protecting the 'right to be forgotten' in the age of blockchain

October 31, 2018 5:56am AEDT

A new framework gives you full administrative control of your blockchain-stored data. Shutterstock

Email

Twitter

Facebook

LinkedIn

Print

46

96

There's been a lot of hype about blockchain over the past year. Although best known as the technology that underpins Bitcoin, blockchain is starting to disrupt other industries, from [supply chains](#) to [energy trading](#).

One of the key selling points of blockchain is that once data is added to the chain, it can't be changed or removed. This makes blockchain trustworthy.

But this same immutability makes blockchain problematic in a world where privacy laws require companies to delete your data from databases once it has served its purpose. This is

Authors



Raja Jurdak

Research Group Leader, Distributed Sensing Systems @ Data61, CSIRO



Ali Dorri

PhD student, UNSW



Salil S. Kanhere

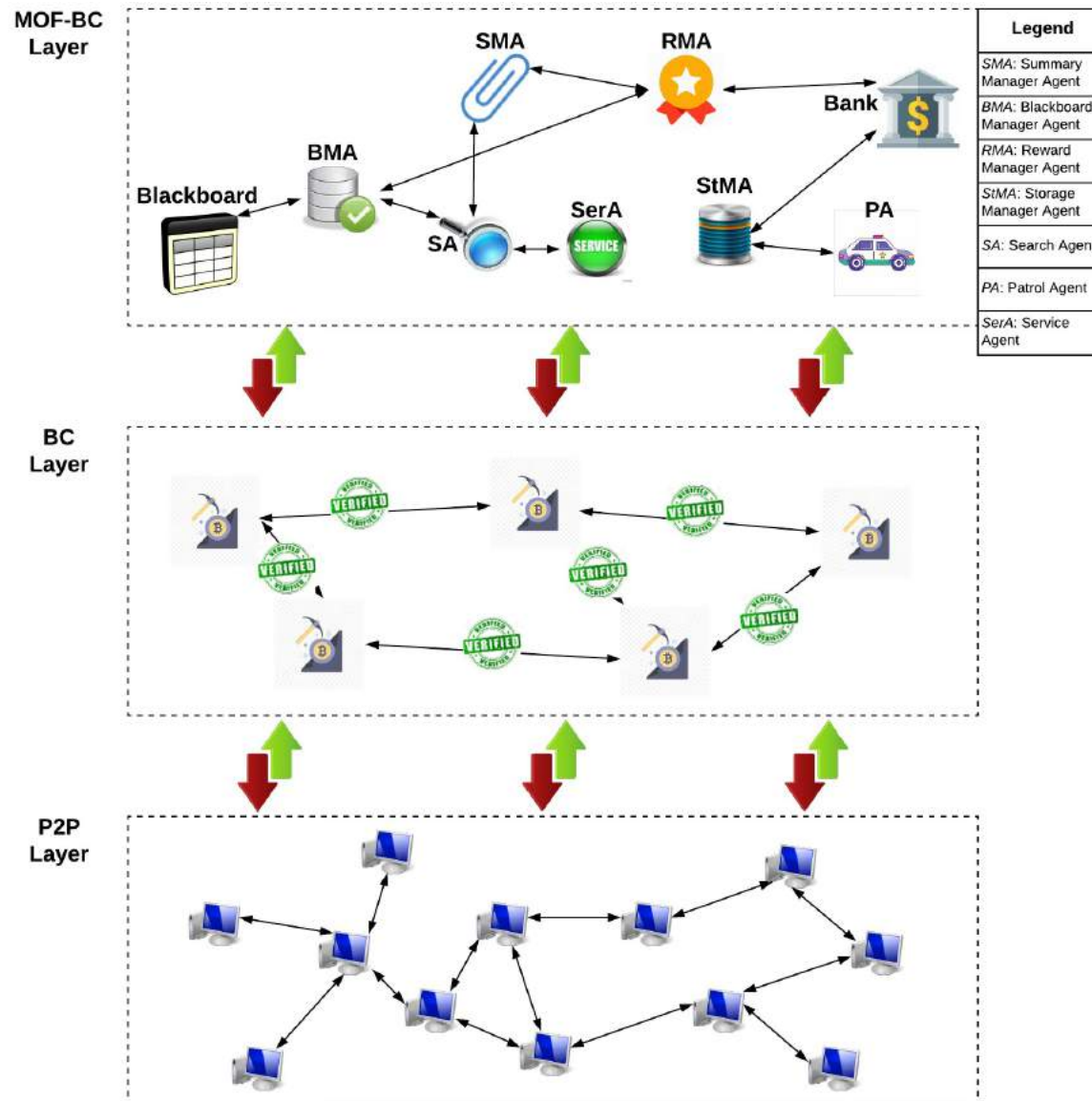
Associate professor, UNSW

Memory Optimized and Flexible BlockChain (MOF-BC)

- Removable blockchain compatible with all existing blockchain instantiations
- User to exercise the right to be forgotten while maintaining blockchain consistency
- Reduces blockchain storage requirements and management costs
- Maintains a level of auditability even if transactions are removed

A. Dorri, S.S. Kanhere, R. Jurdak, A Memory Optimized and Flexible BlockChain for Large Scale Networks, Future Generation Computer Systems, Volume 92, Pages 357-373, March 2019.

MOF-BC Architecture



MOF-BC: Keeping transaction hashes consistent

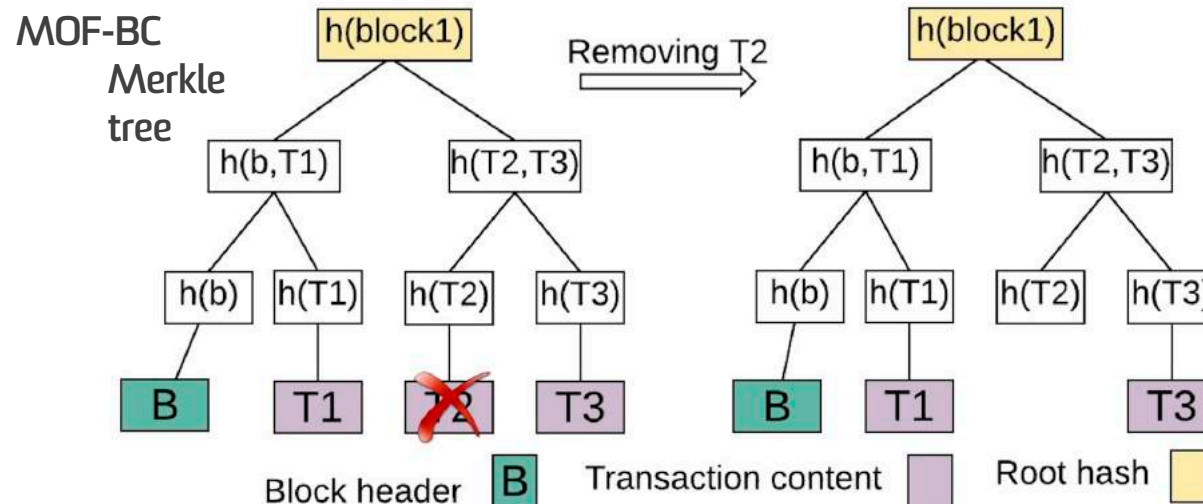
To keep blockchain consistency maintain the hash of a transaction and remove its content.

$$Block_{ID} = H(T_1 || T_2 || \dots || T_k || block.header)$$

Conventional BCs

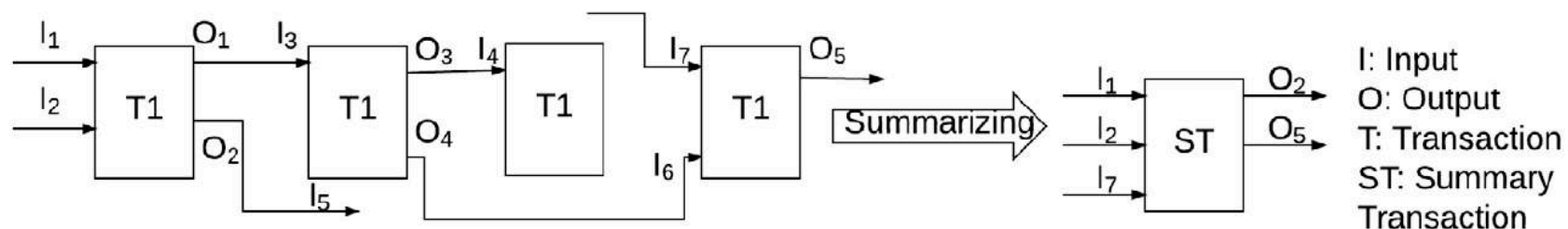
$$Block_{ID} = H(T.ID_1 || T.ID_2 || \dots || T.ID_k || H(block.header))$$

MOF-BC



MOF-BC: Memory Optimization Modes 1/2

- Temporary
 - A transaction is stored for a specific period of time
- Summarizable
 - Multiple transactions are summarized in one transaction
 - The summarized transaction contains the root hash of the Merkle tree built using the hash of summarizing transactions
 - Inputs are summarized as below:



MOF-BC: Memory Optimization Modes 2/2

- Aging
 - The data stored in the cloud can be optimized
 - The corresponding original transaction is redirected to a new transaction
 - A blockboard maintains the ID of the redirections
- Permanent
 - A transaction is stored in blockchain for ever (similar to existing blockchains)



*forever
and
always*
♡

MOF-BC: Incentives



Introduces *storage fee*:

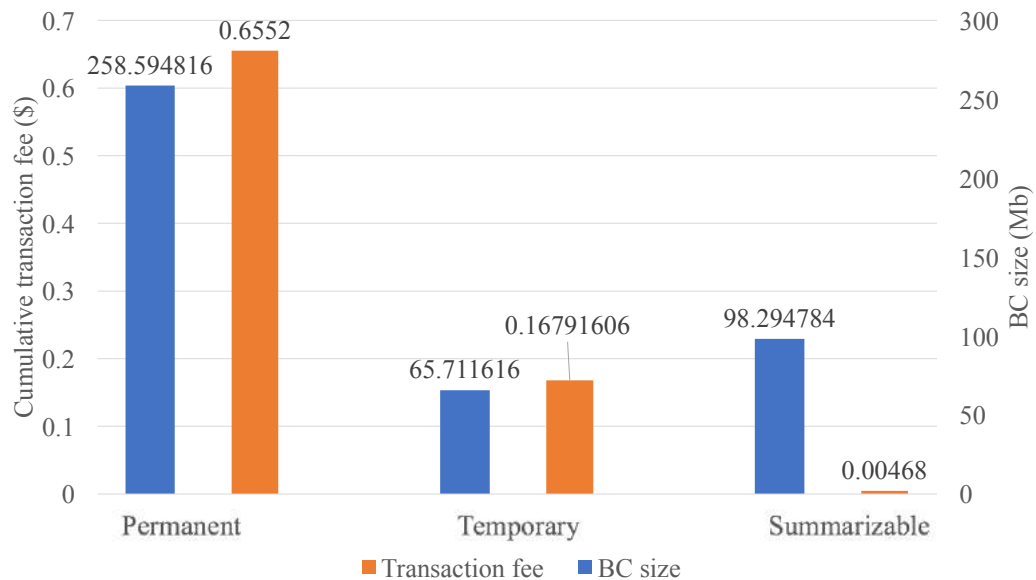
- Storage fee is based on size of transaction
- Each node that stores blockchain is paid depending on the storage space allocated to the blockchain

$$Share_X = Storage_X * \frac{Fee}{Store_{All}} * \frac{Time_X}{PaymentPeriod}$$

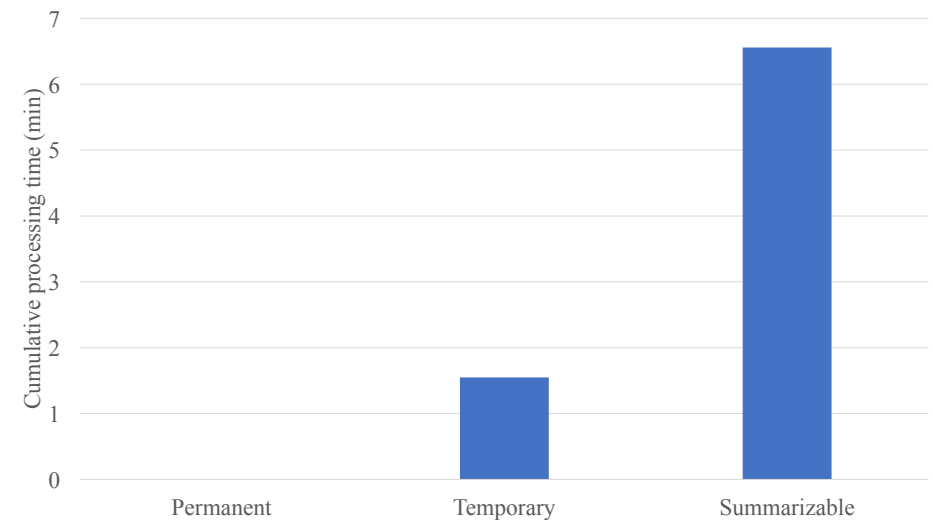
Motivates users to remove their transactions by offering rewards

Introduces batch removal of transactions (cleaning period) to reduce the processing time overhead on nodes

Performance Evaluation



Cost vs. Storage



Processing

Performance Evaluation



Table 5

The saved and incurred cost by MOF-BC (\$).

	Temporary	Summarizable
Saved cost	0.48728394	0.65052
Incurred cost	0.000374948	0.001586572
Benefit/Cost ratio	1300	410

2

SUPPLY CHAINS





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.

WorldViews

Australia searches for culprit hiding sewing needles in strawberries

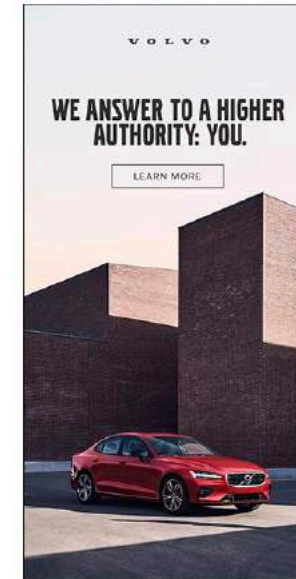


Fresh ripe strawberries in boxes for sale at a market. (iStock)

By **Siobhán O'Grady**

September 17

It's a crime so strange that any motive seems nearly inconceivable: In Australia, someone is placing sewing needles inside strawberries — endangering those who eat them and sending panic across strawberry markets as prices plummet and government officials scramble to find a culprit.



Food Safety

Food Borne Infections

- Salmonella Outbreak 2017
- 235 people fell sick across 26 states
- linked to imported Maradol papayas
 - **took two months** to identify the source of contamination

Food Fraud

- substitution, tampering, misrepresentation
- Ex. 2013 UK horse meat scandal, 2008 China milk scandal

Illegal Production

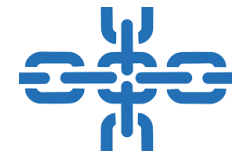
- ~10-22% of total global fisheries production is unreported/unregulated

Food Recall/Loss

- Average cost of recall to company: \$10 million

Origin
Quality
Handling





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
 - Centralized
 - Prone to mishandling, counterfeiting
 - Consumer access to data often not available or incomplete



Honest 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

Challenges

Type of Blockchain

- public blockchain – not suitable for business processes and complexities of supply chain

Defining Permissions

- Access on the ledger

Scalability of Blockchain

- Scalable network architecture

Consumer Access to traceability information

- Consumer access to public information

What is needed?

A holistic framework that addresses the above

Challenges

Type of Blockchain

- public blockchain – not suitable for the complexities of supply chain

Permissioned Blockchain,
Transaction Vocabulary

Defining Permissions

- Access on the ledger

Consortium: FSC participants, Governing Bodies
Defining Access Controls

Scalability of Blockchain

- Scalable network architecture

Network Architecture: Sharded

Consumer Access to traceability information

- Consumer access to public information

On shelf access through
customized BC explorers

Contributions

- **Permissioned blockchain architecture**
- **Consortium Model** to govern permissions to the ledger
- **Transaction Vocabulary**
 - Improved writing accessibility to the ledger
 - Each Food Supply Chain (FSC) participant has a well-defined role
- **Scalable Network Architecture**
 - Use Sharding
- **Access Control List**
 - Hide trade flows, limit read/write access to ledger

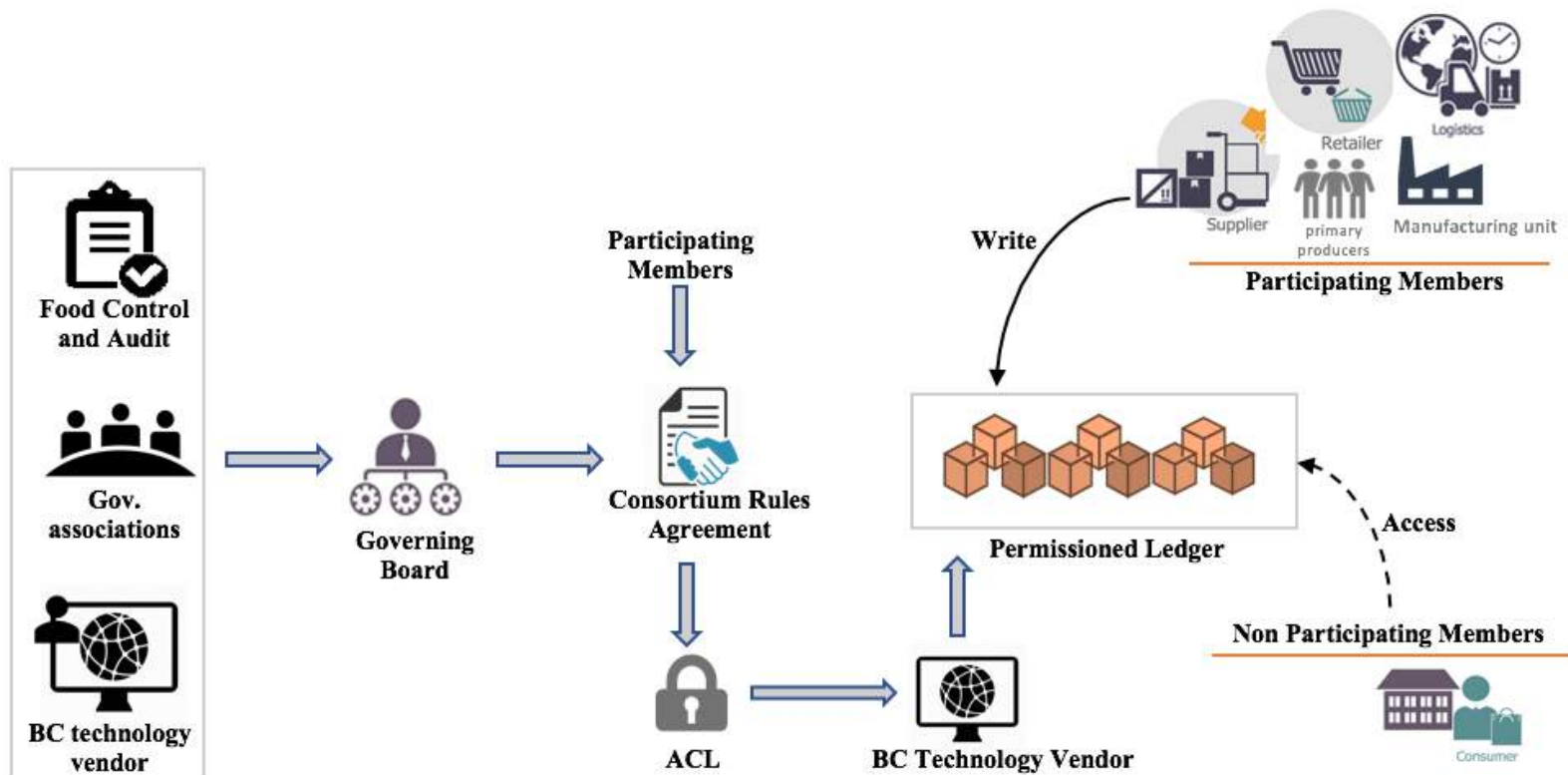
S. Malik, S. S. Kanhere and R. Jurdak, "ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains" in Proceedings of the IEEE Symposium on Network Computing and Applications (IEEE NCA), Boston, November 2018.

Consortium

No Single FSC participant dominates

- Access Rules

Regulatory and Government associations such as FSANZ, ACCC



Permissioned Network based on Sharding

Permissioned blockchain –scales to only a few hundred nodes

Sharding - a single blockchain by interconnecting multiple independent side chains.

A Side Chain

Operational area of FSC in single geographical area

Permissioned Access

A local private blockchain for a side chain

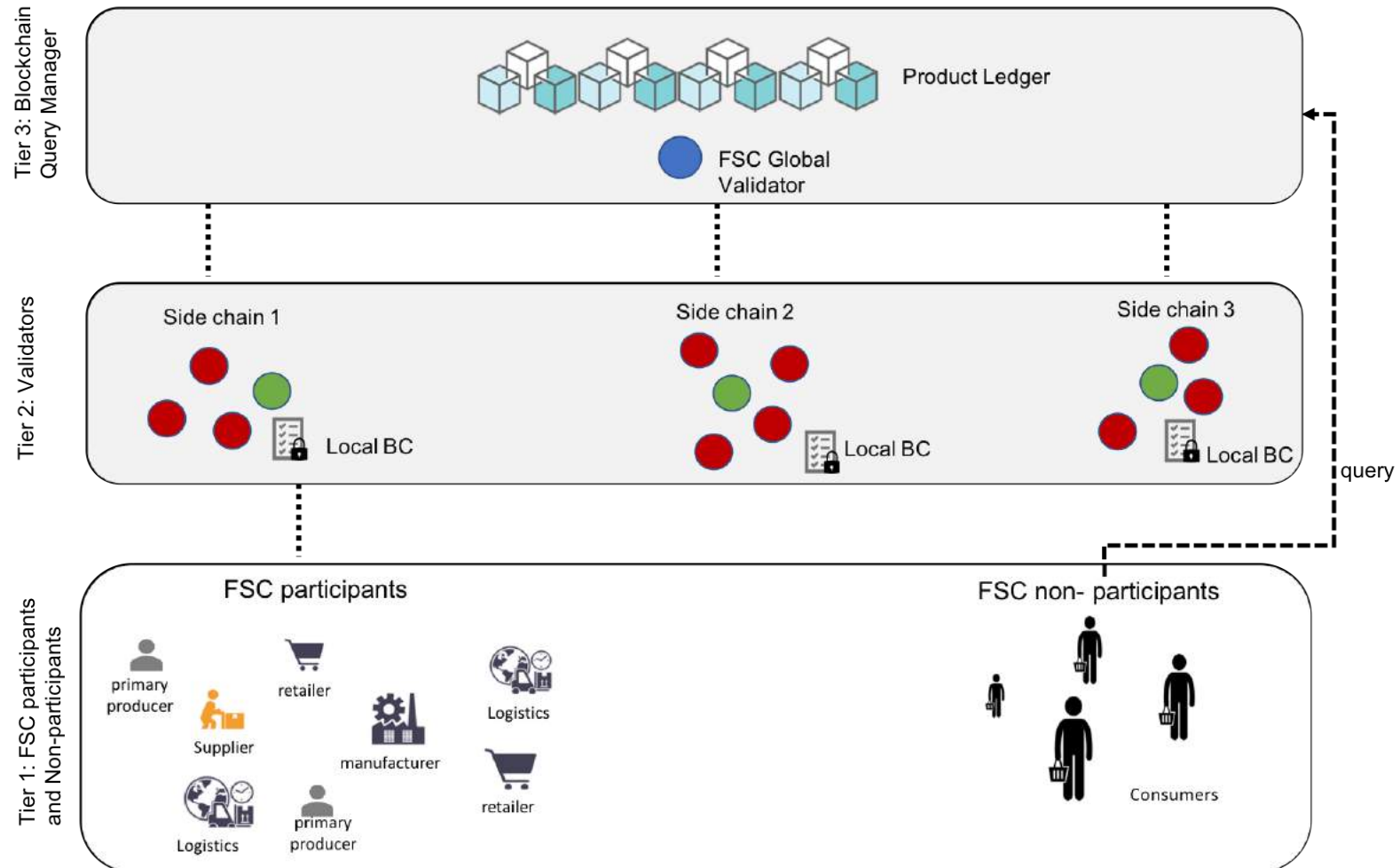
‘Write’ operations from FSC participants

Public Access

A global blockchain – stores local ledger from each side chain

Serves as Query manager for restricted read access

Network Architecture

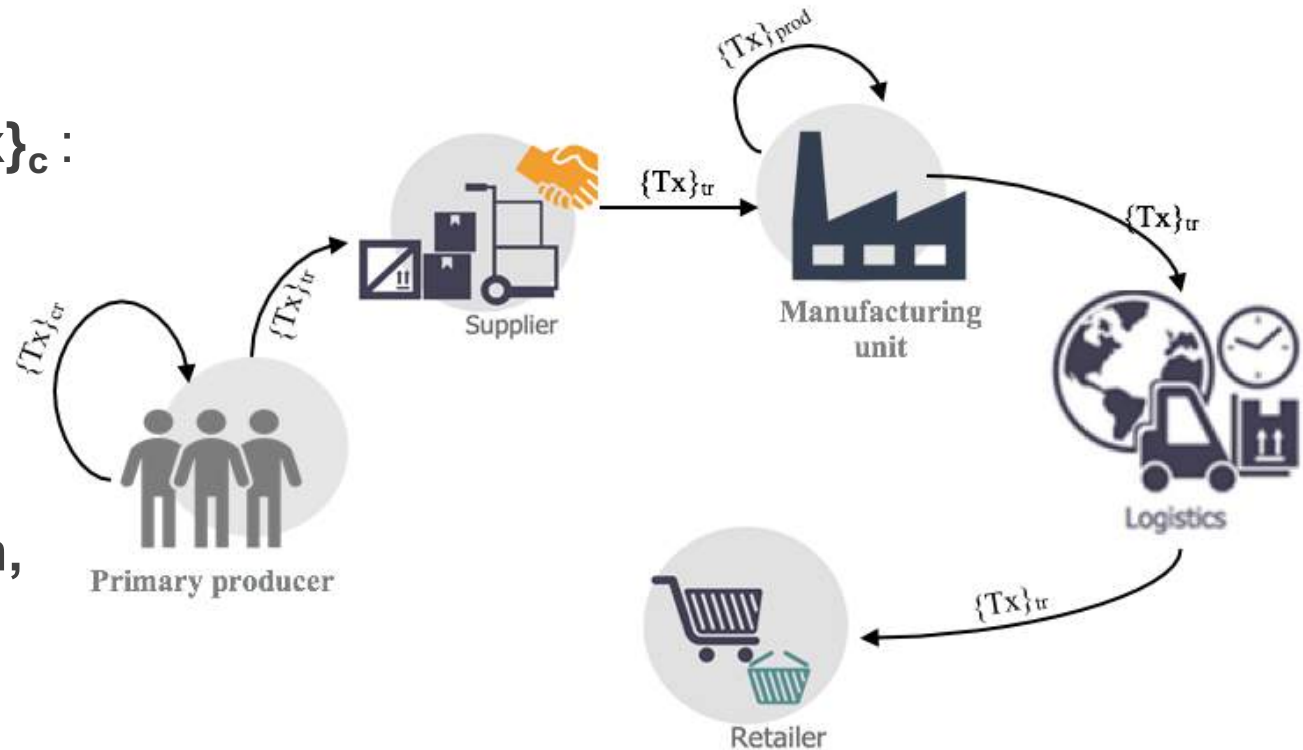


Transaction Vocabulary

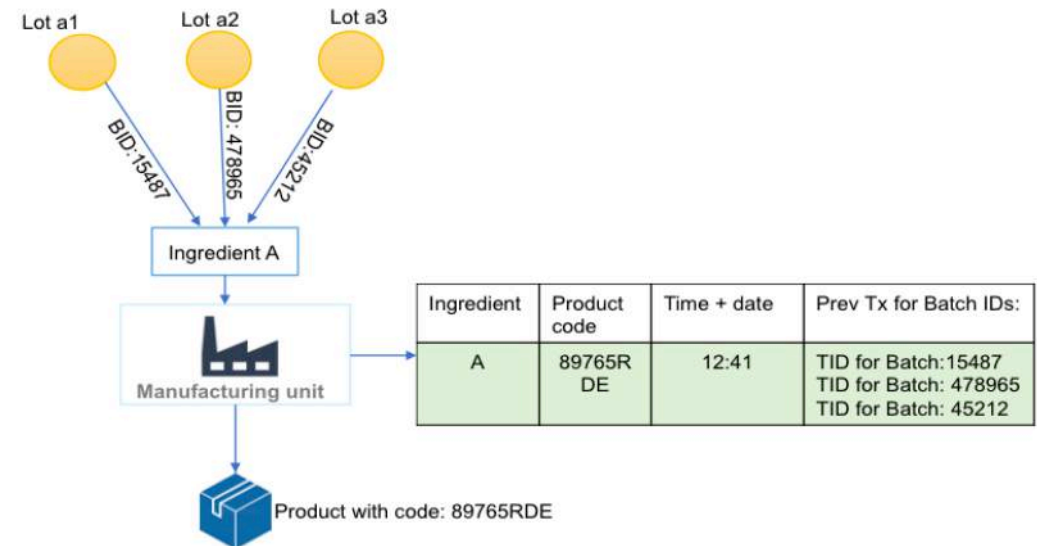
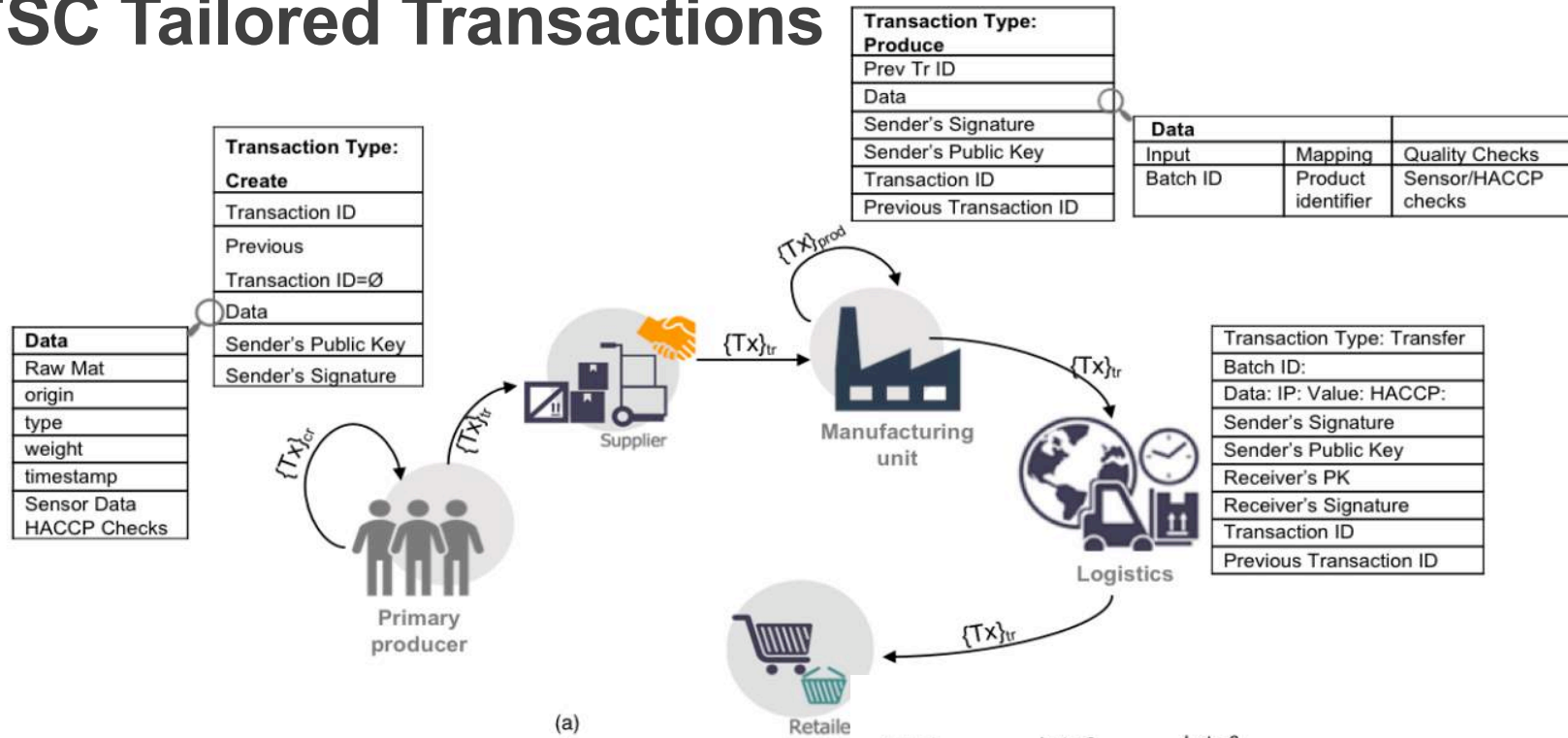
Create Transaction, $\{Tx\}_c$:
uni-sig

Transfer Transaction, $\{Tx\}_{tr}$:
multi-sig

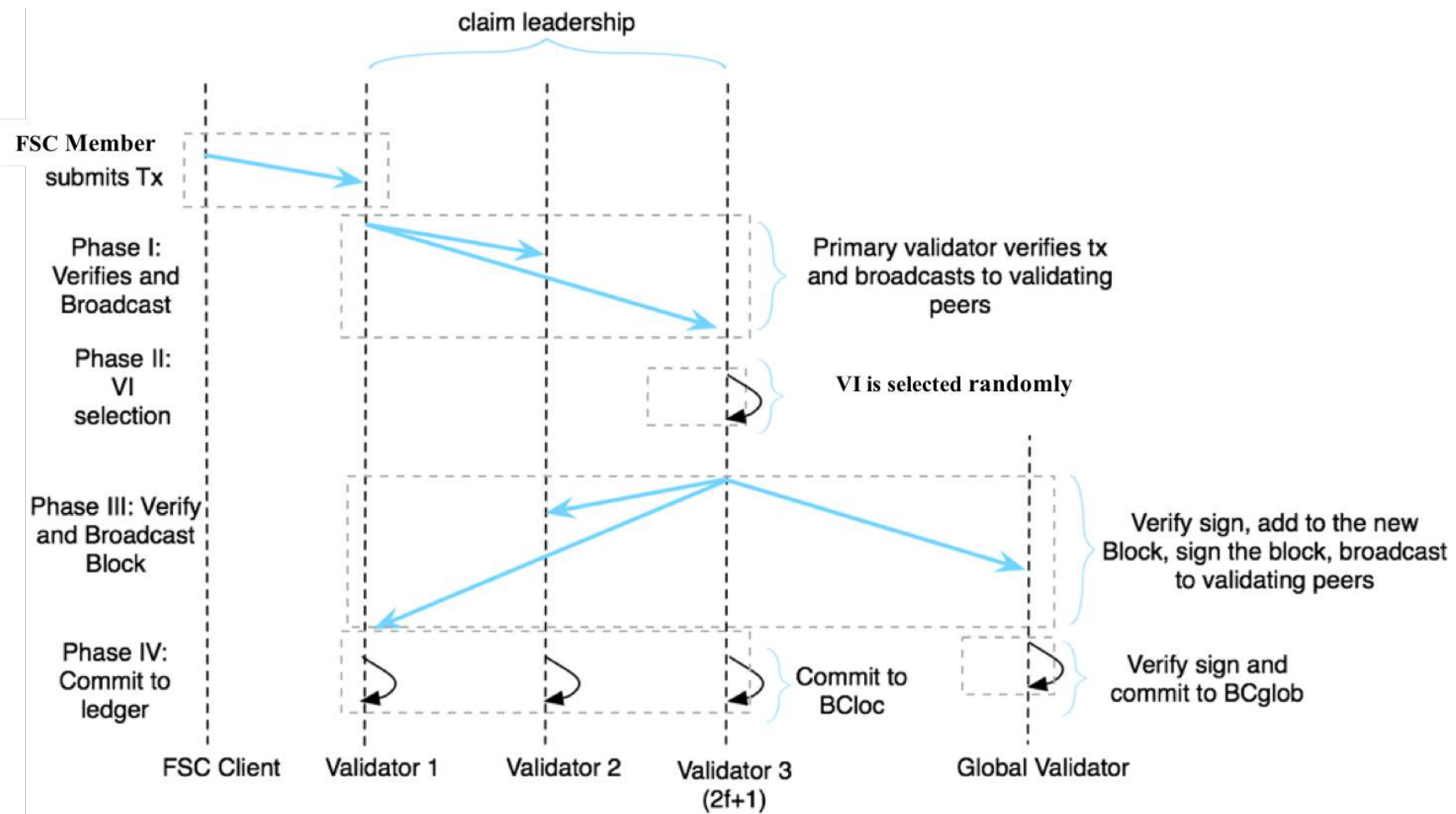
Production Transaction, $\{Tx\}_p$:
uni-sig



FSC Tailored Transactions



Consensus



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

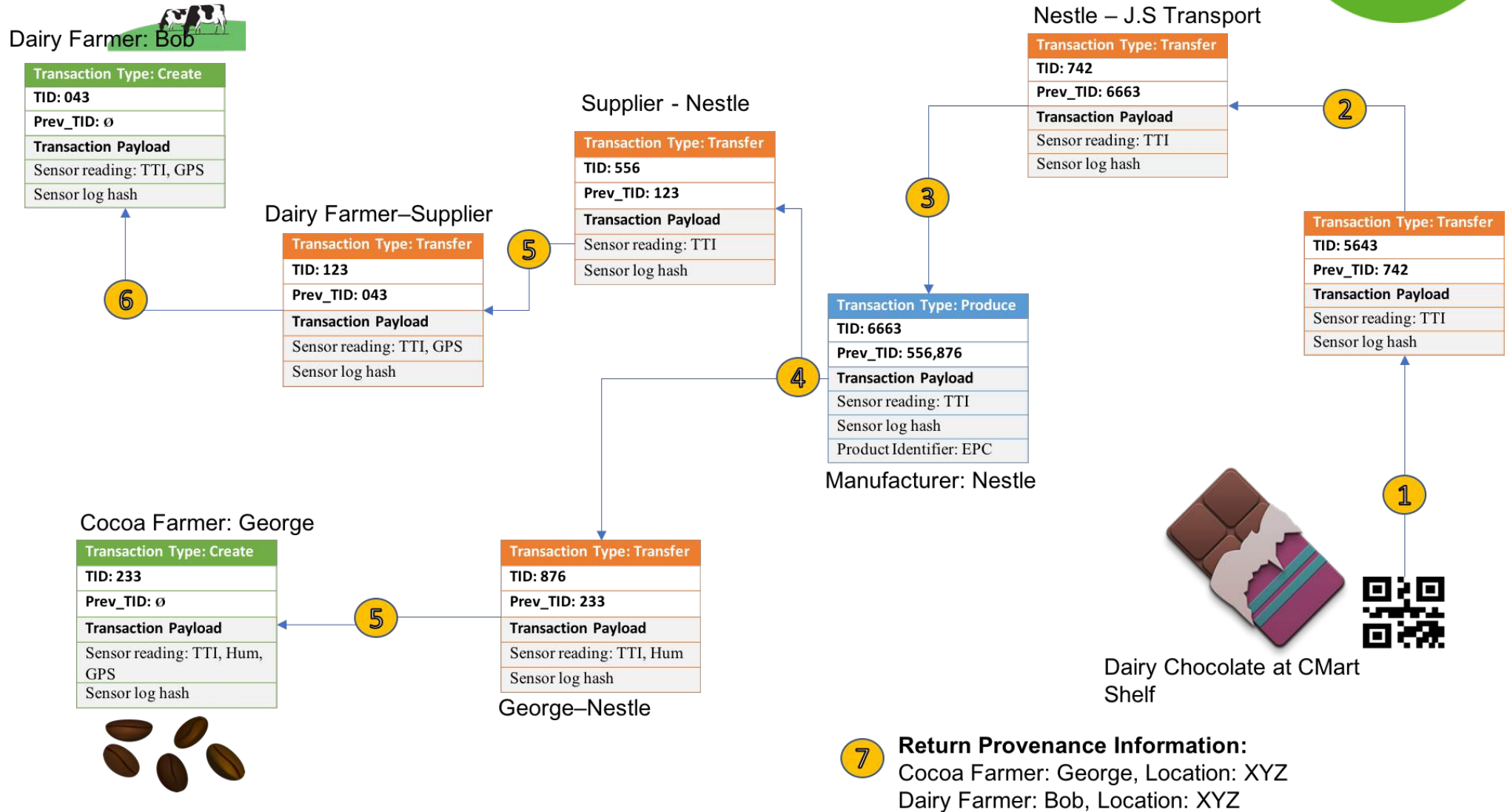
Security Analysis

Attack	Description	Primary Targets	Attack Likelihood	Adverse Effects	Possible Countermeasures
Double Transfer	a dishonest FSC participant broadcasts the same Tx for multiple asset transfers	buyers	unlikely	A buyer signs TX_{tr} for which physical asset does not exist	Every Tx is coupled with physical trade of goods, ensuring no double trade
DOS/DDOS Attack	attacker floods the validator node with invalid TXs	validators	unlikely	deny services to honest users	TX is only relayed if it is from a valid participant and thresholding methods are used to limit TXs
Wallet theft	stealing or destroying private keys of FSC participants	participants	unlikely	FSC participant loses keys	Security support from CA, also adversary cannot issue TXs in absence of physical asset.
Sniffing Attack	Attacker seeks to analyze the transaction traffic generated by a participant to obtain insights about their trades	participants	likely	trade frequency exposed to potential competitor	TOR integration to conceal user IDs and encryption of data field in Txs
Sybil Attack	an attacker creates multiple identities of participants to take control of system	BC network	not applicable	DOS attacks ans users' privacy	permissioned access to only pre-registered participants
ID Spoofing	an attacker impersonates as a legitimate participant by replicating a public key	participants	unlikely	trade on behalf of participant	Tx will require signatures(private key) hence Tx would not be considered valid.
51% Attack	an adversary controls more than 51% of the validators	BC network	not applicable	generate fake blocks, delay block validation	we assume BTV deploys a trusted network resilient to insider attacks and uses state of the art IDPS.
Spamming Attack	spamming queries with fake TID	BC explorer	likely	launch DOS attacks	security metrics for web APIs such as CAPTCHA

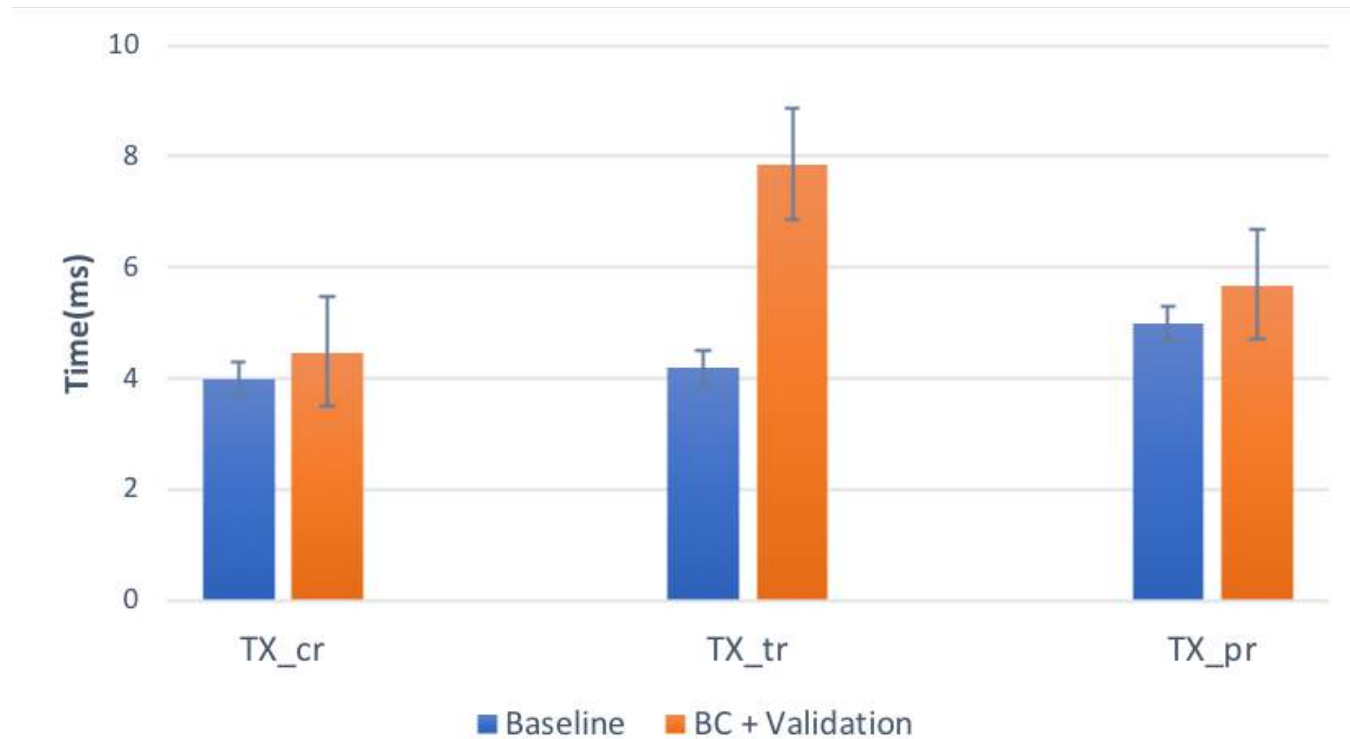
Experimental Setup

- Designed and Implemented a permissioned blockchain
 - **Programming Language and Tools**
 - Python, SQLite, CORE
 - Python PyCrypto – cryptographic library
 - **Network**
 - Client-Server
 - **Evaluation Parameters**
 - Querying Provenance
 - Validation time
 - Query time

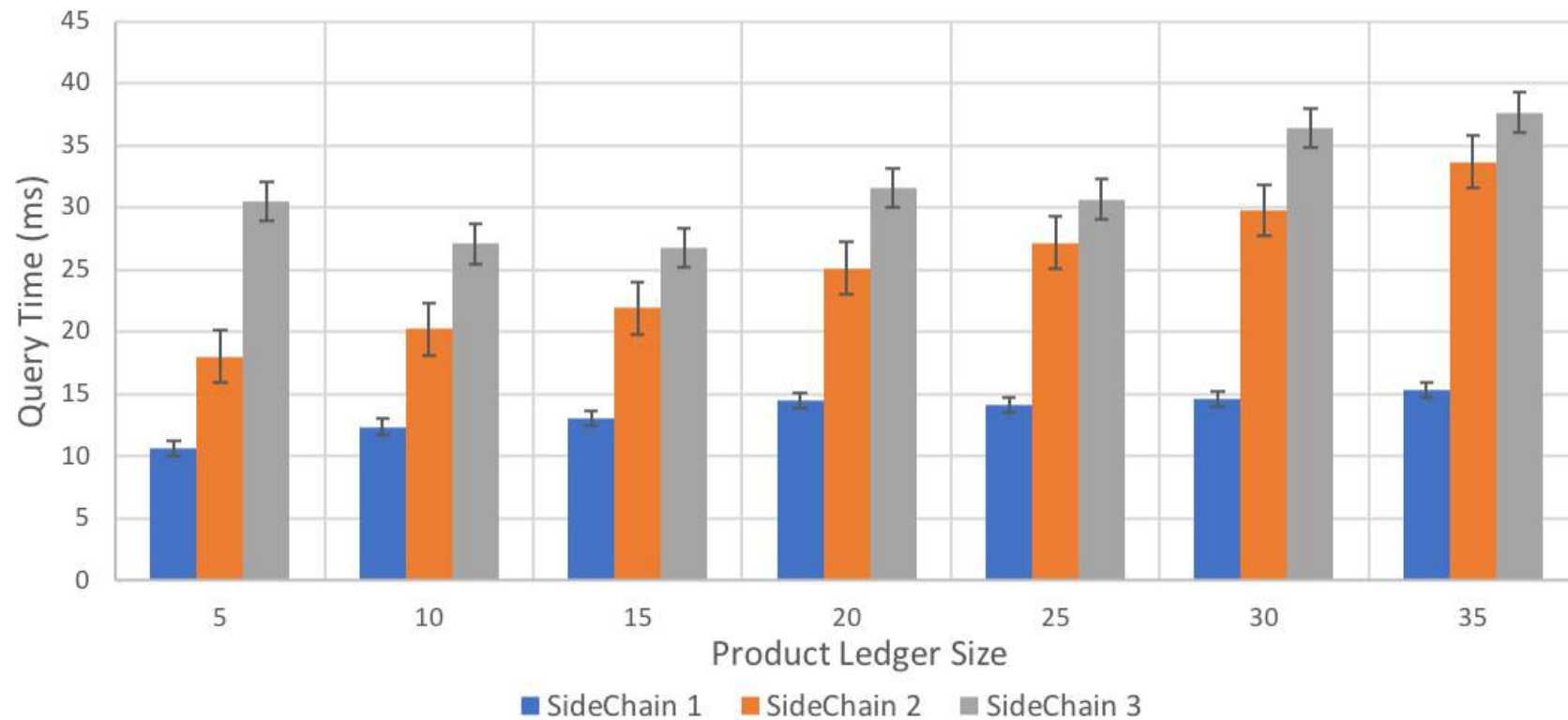
Querying Provenance



Results: Transaction Validation Time



Results: Query Time



Trust?



How do we trust data written into the blockchain?

- Hashed data on the blockchain represents physical observations of physical events

Need for a trust management system with the following requirements

- Multi-faceted assessment of trustworthiness of logged data which incorporates inputs from IoT sensors, feedback provided by supply chain entities, physical audits, etc.
- Flexibility for ascribing trust to the supply chain entities and commodities and also at different granularities
- Automation of various processes – reputation computation, rewards, penalties
- Minimal overheads

TrustChain

BC-based reputation/trust framework

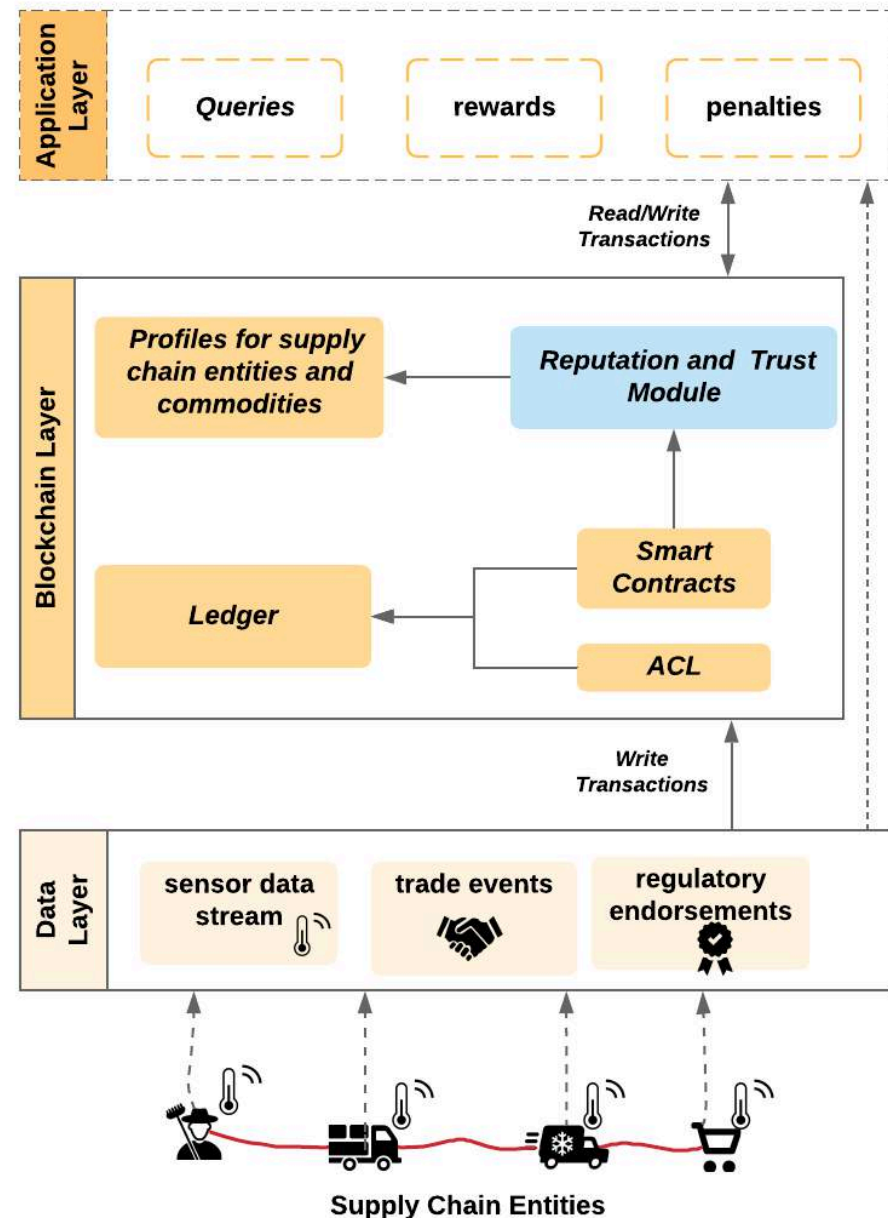
Flexible and granular

Smart contracts for automation

Accountability mechanisms

Hyperledger Fabric Implementation

Minimal overheads



S. Malik, V. Dedegoulu, S. S. Kanhere, and R. Jurdak,
“TrustChain: Trust Management in Blockchain and IoT supported
Supply Chains”, under review.

Data Layer: Transactions

Data Observations

- **Sensors:** Continuous temperature monitoring

$$TX_{sens} = [CID|H_{data}|Sig_{device}]$$

- **Regulatory bodies:** Physical inspection of the storage facility

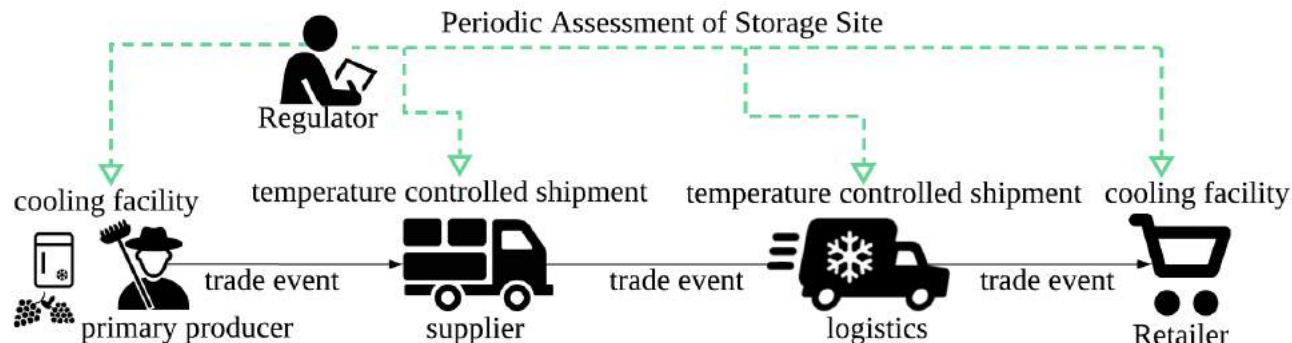
$$TX_{Reg} = [ID_s|H_{data}|C_{type}]$$

- **Traders:** Satisfaction of trade with each other

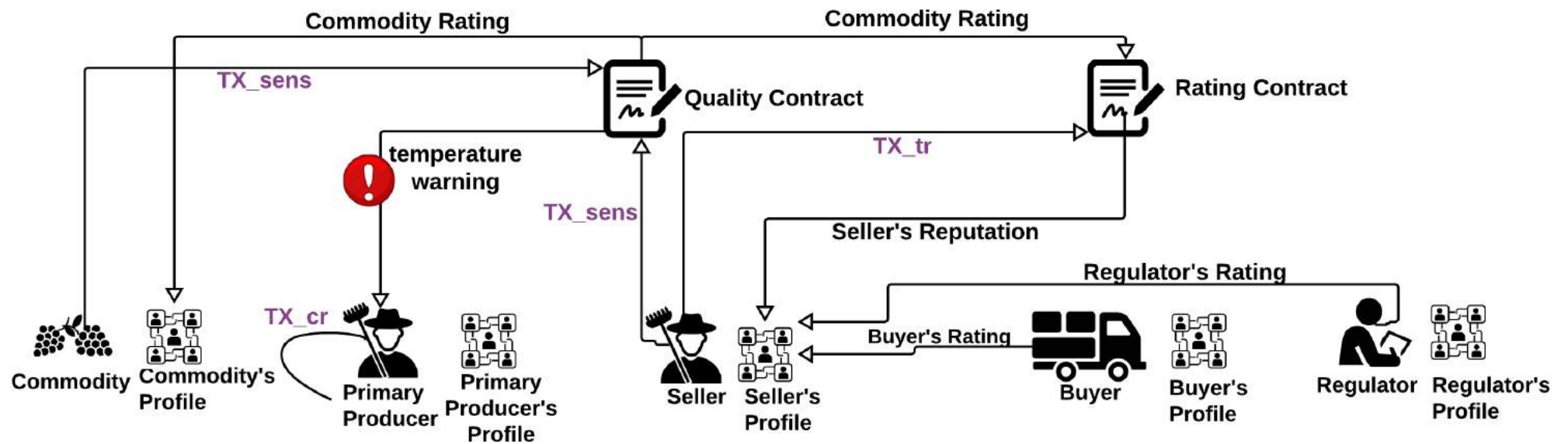
$$TX_{cr} = [CID|H_{data}|ID_o|ID_{contract}|Sig_o|PU_o]$$

$$TX_{tr} = [CID|H_{data}|ID_b|Sig_s|PU_s|Sig_b|PU_b]$$

$$TX_{rec} = [CID|Sig_r|PU_r]$$



BC Layer: Smart Contracts



BC Layer: Reputation and Trust Module

Commodity's Reputation

$$Rep_{sens} = [Rep_{sens}(t_0), Rep_{sens}(t_1), \dots, Rep_{sens}(t_{n-1})]$$

Seller's Reputation

$$Rep_{seller} = w_1 \times Rep_{sens}(t) + w_2 \times Rep_{trader}(t) + w_3 \times Rep_{reg}(t)$$

$$R(t_n) = \sum_{t=t_0}^{t=t_n} Rep_{seller}(t) \times \beta(t_n - t)$$

Seller's Trust

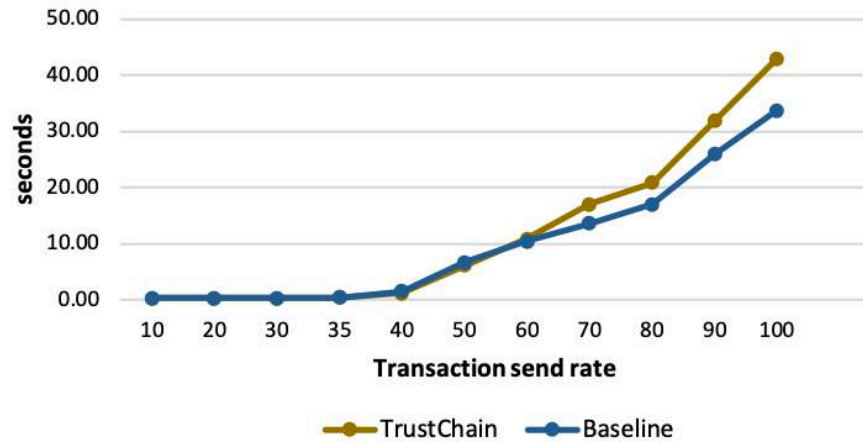
$$T_{trader}(t_n) = \alpha_0.R(t_n) + \alpha_1.f_1 + \alpha_2.f_2 + \dots + \alpha_N.f_N$$

TRUST FEATURE AND FEATURE SCORE

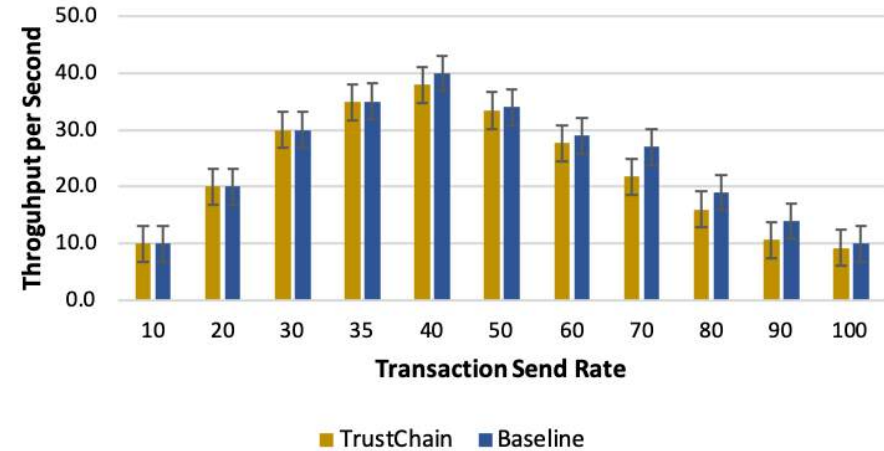
Number of Successful Transactions	Feature Score (f_1)
0	-1
1-3	0.5
4-6	1.5
≥ 6	2

Results

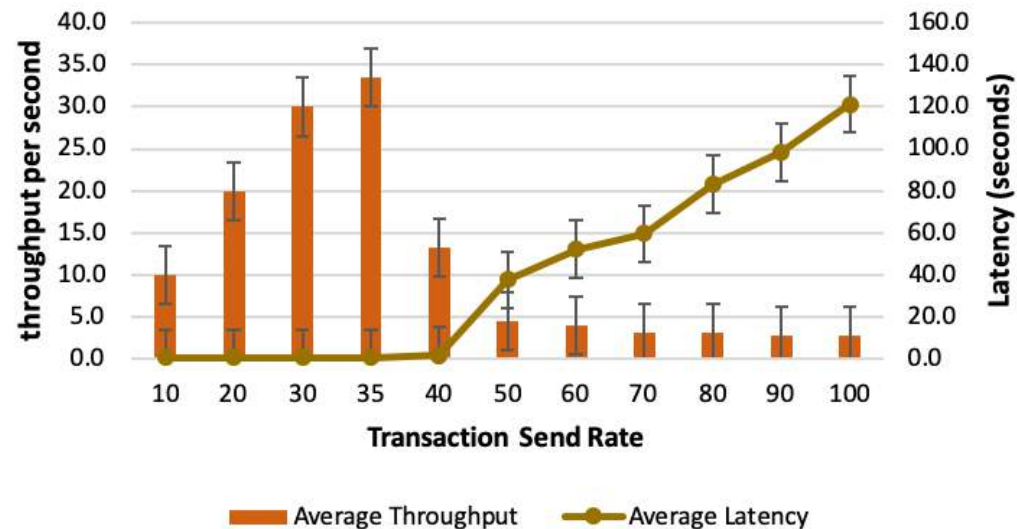
Trade Transaction-Latency



Trade Transaction - Throughput



Create Transaction

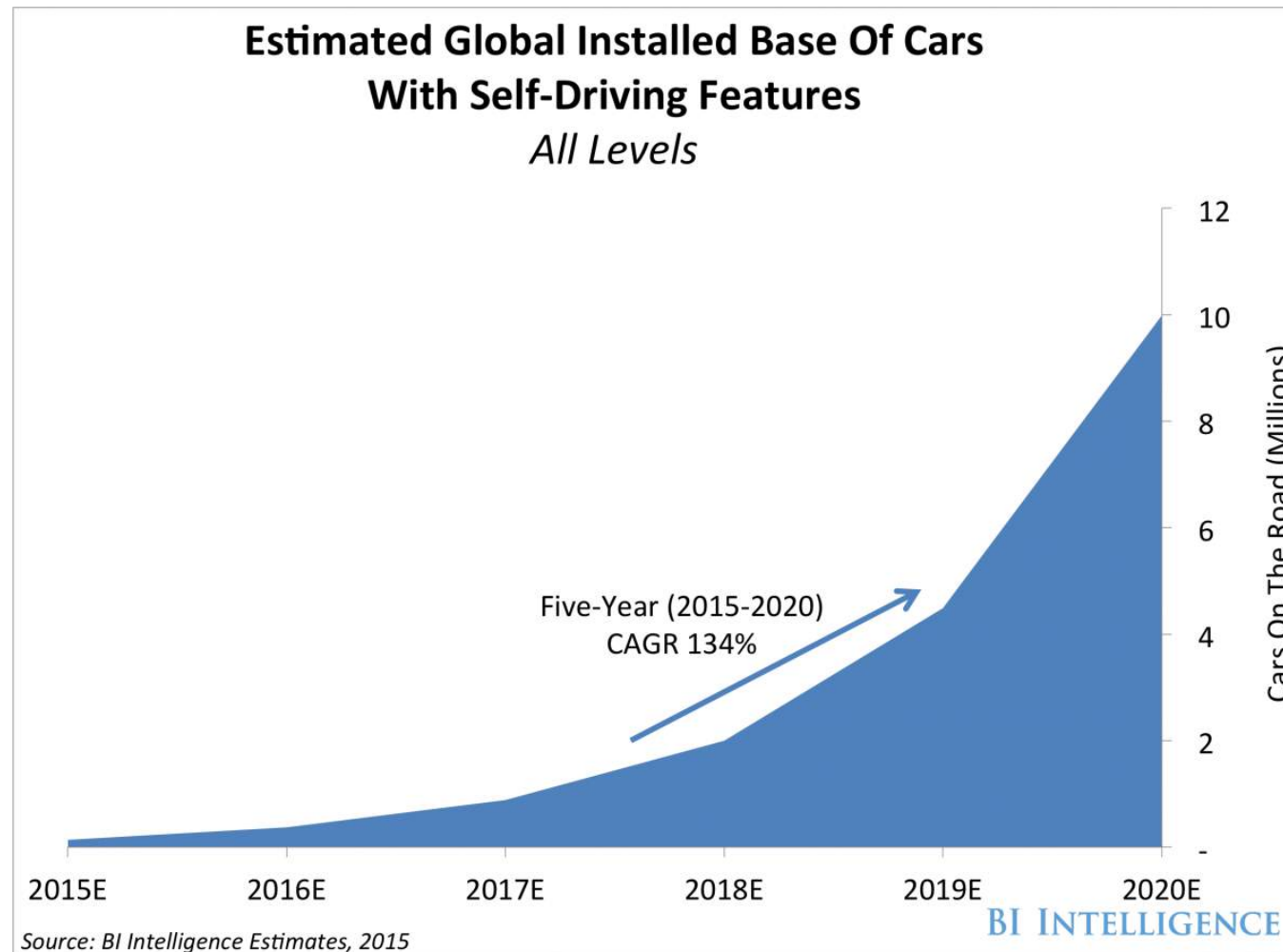


3

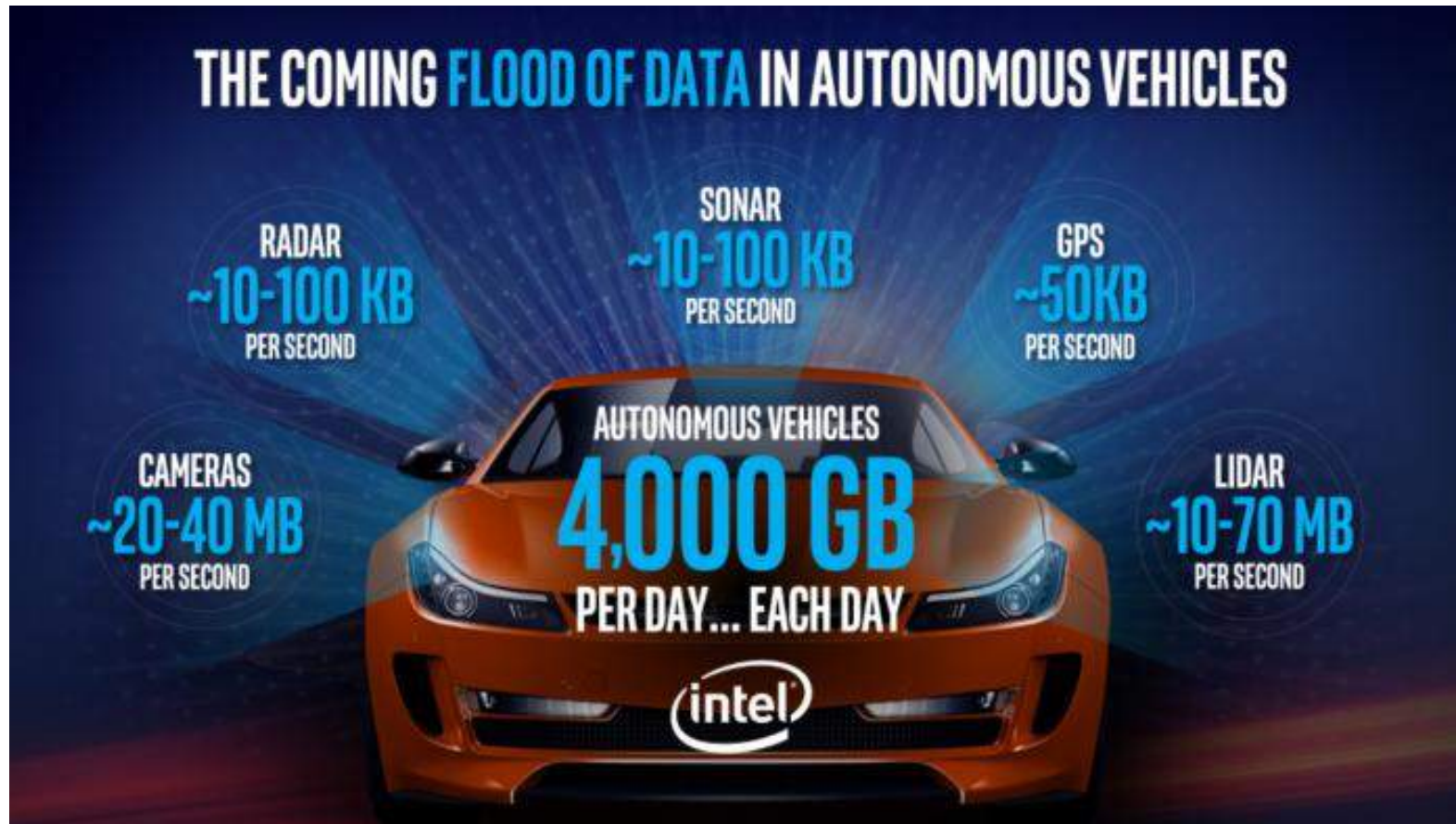
CONNECTED VEHICLES



Connected and Automated Vehicles (CAVs)



Connected and Automated Vehicles



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

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

SHARE



SHARE
208411



TWEET



COMMENT



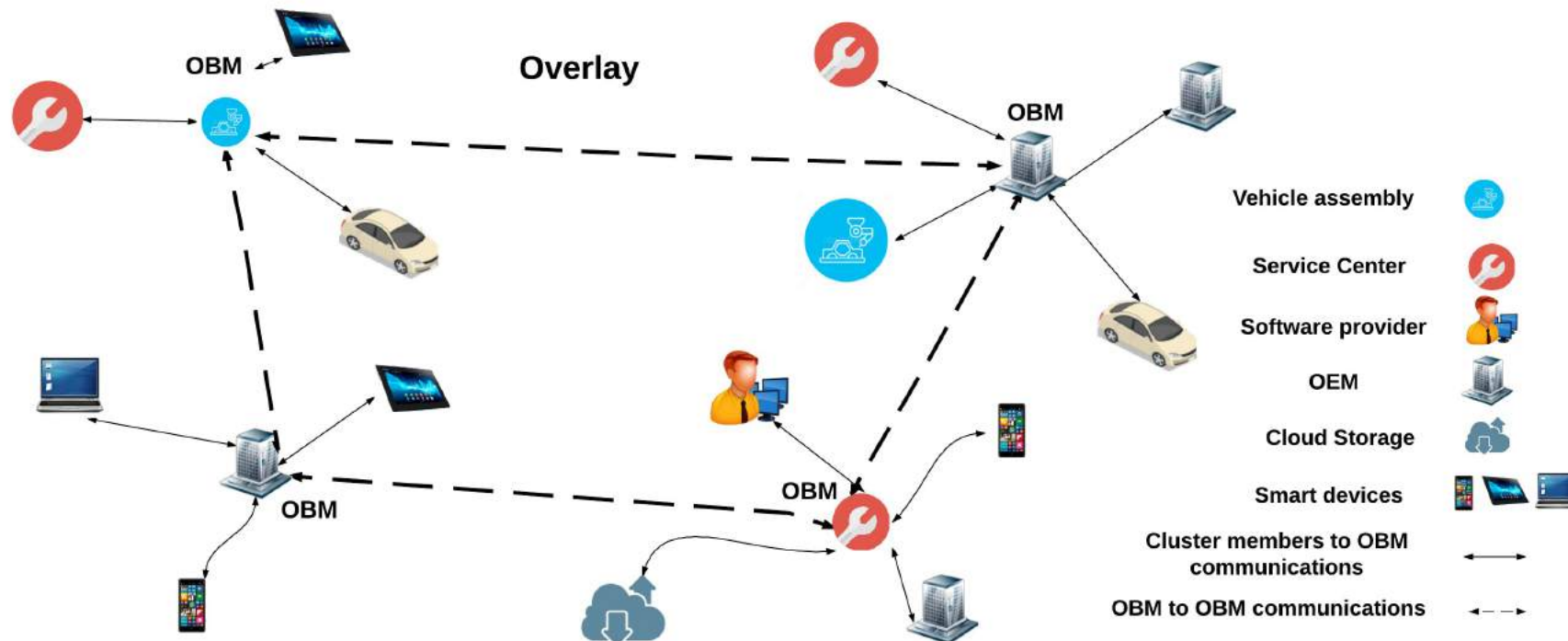
EMAIL

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



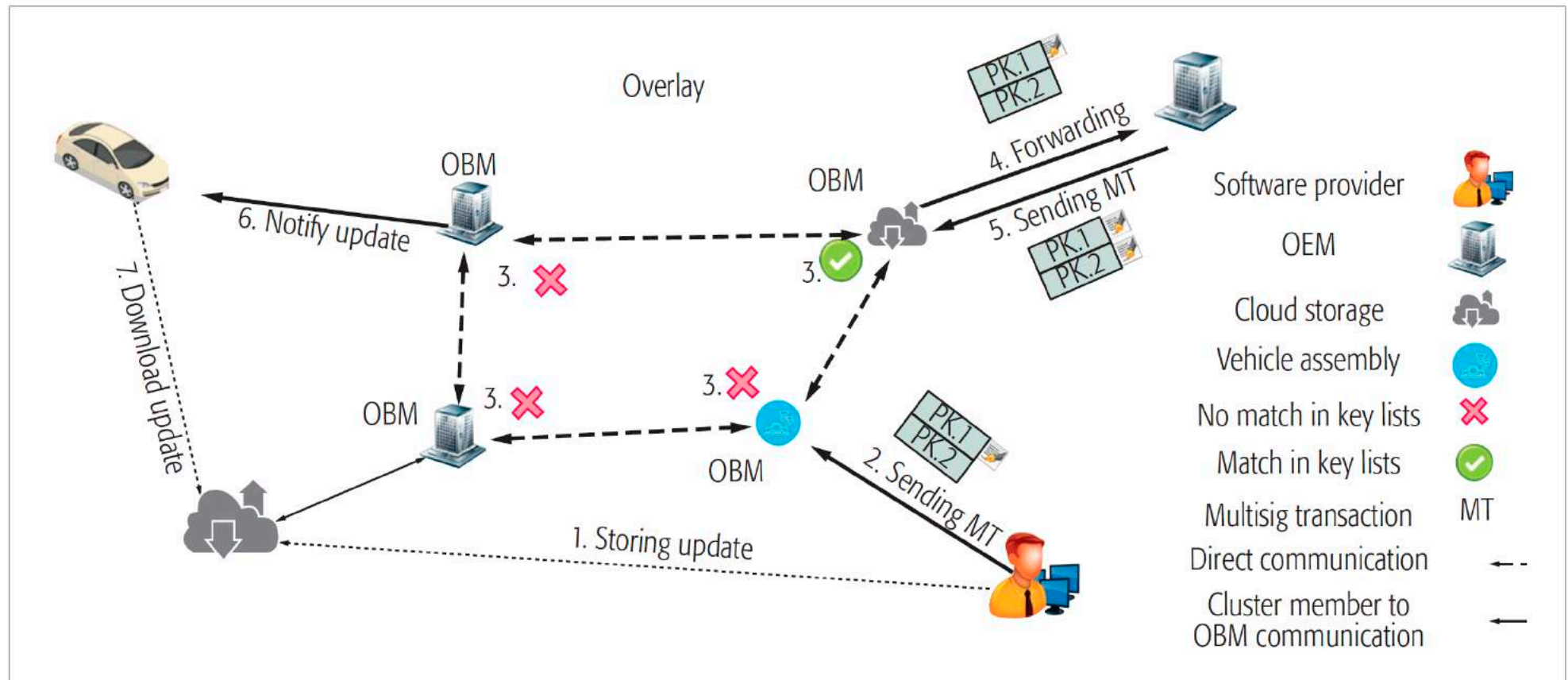


Blockchain for Automotive Security and Privacy



A. Dorri, M. Steger, S. Kanhere, and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy", IEEE Communications Magazine, Volume 55, Issue 12, pages 119-125, December, 2017.

Wireless Remote Software Update



Insurance



- Insurance company and the user share a key pair when signing contract
- The user uses the key to share data with the insurance company
- The privacy-sensitive data of the user is stored in an in-vehicle storage and only the hash of the data is stored periodically in blockchain
- Once requested the user can share data and insurance company can ensure integrity of the data by comparing the hash

Blockchain for Automotive Security and Privacy

Application	Conventional methods	Advantages introduced by BC
WRSU	<ul style="list-style-type: none"> • Centralized – not scalable • Partial participation: not addressing the full chain starting from a SP all the way to a service center • Lack of privacy: a direct link between the vehicle and OEM can compromise the driver's privacy (e.g., driver behavior or location) • Only an OEM can verify communications or history of update downloads. 	<ul style="list-style-type: none"> • Distributed data exchange and security provides scalability • End-to-end: involving SP, OEMs, vehicles, service centers, assembly lines, and so on • Ensure privacy of the user (also for diagnostics) • Update history as well as authenticity of the software can be publicly verified
Insurance	<ul style="list-style-type: none"> • Current systems are often insecure, which endangers the vehicle's integrity [10] • Users lack control over the exchanged data • Privacy-sensitive data must be continuously sent to the insurance company for receiving services 	<ul style="list-style-type: none"> • Secure, distributed, and privacy-preserving data exchange • Users control the exchanged data • Privacy-sensitive data is shared on demand (e.g., accident happened) instead of a continuous data exchange. Authenticity of data stored in the vehicle can be publicly confirmed
Electric vehicles	<ul style="list-style-type: none"> • Central payment and accounting • The location and behavior (e.g., using a specific charger on a specific day) of the user can be tracked. 	<ul style="list-style-type: none"> • Private and distributed security, payments, and accounting • User data such as location information remain private
Car-sharing services	<ul style="list-style-type: none"> • Central payment and accounting • Users can be tracked by their identity • Central authorization 	<ul style="list-style-type: none"> • Private and distributed security, payments, and accounting • Users use changeable identities • Distributed authorization

Table 1. A summary of BC advantages compared to conventional methods employed for studied applications

Proof-of-Concept

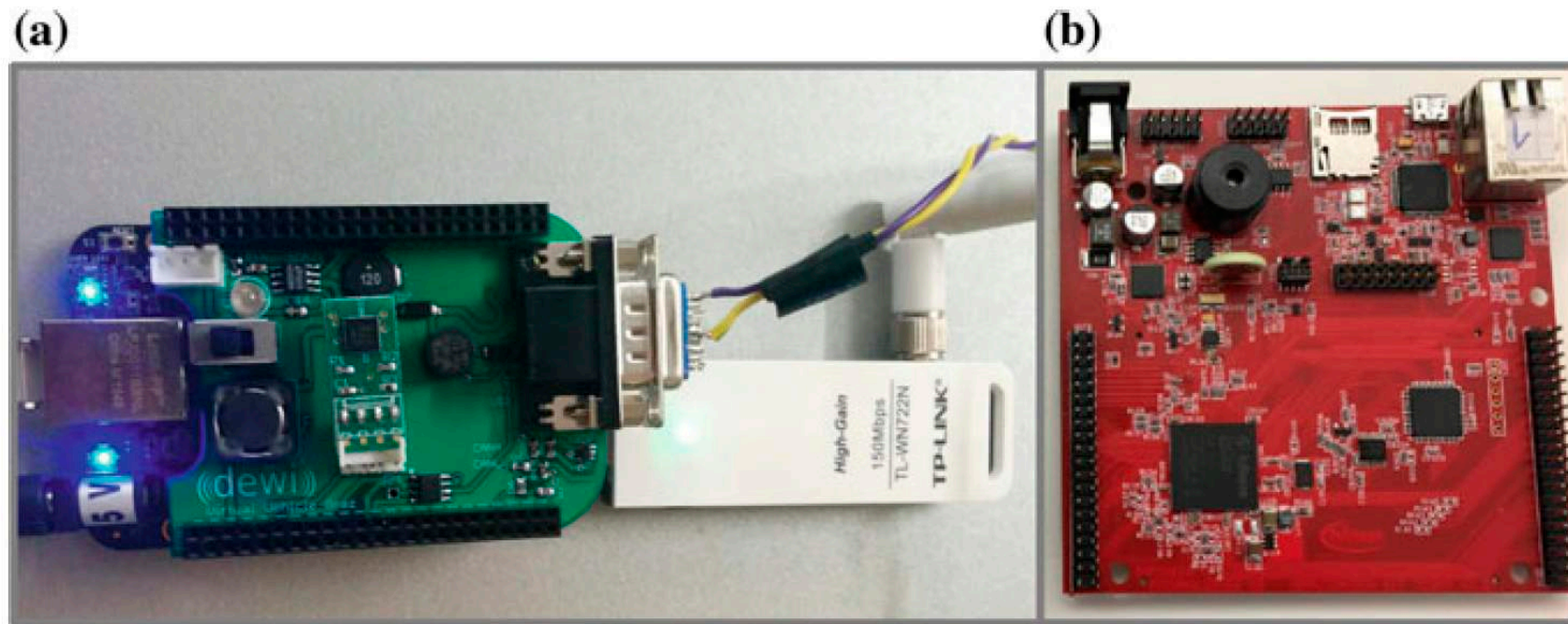
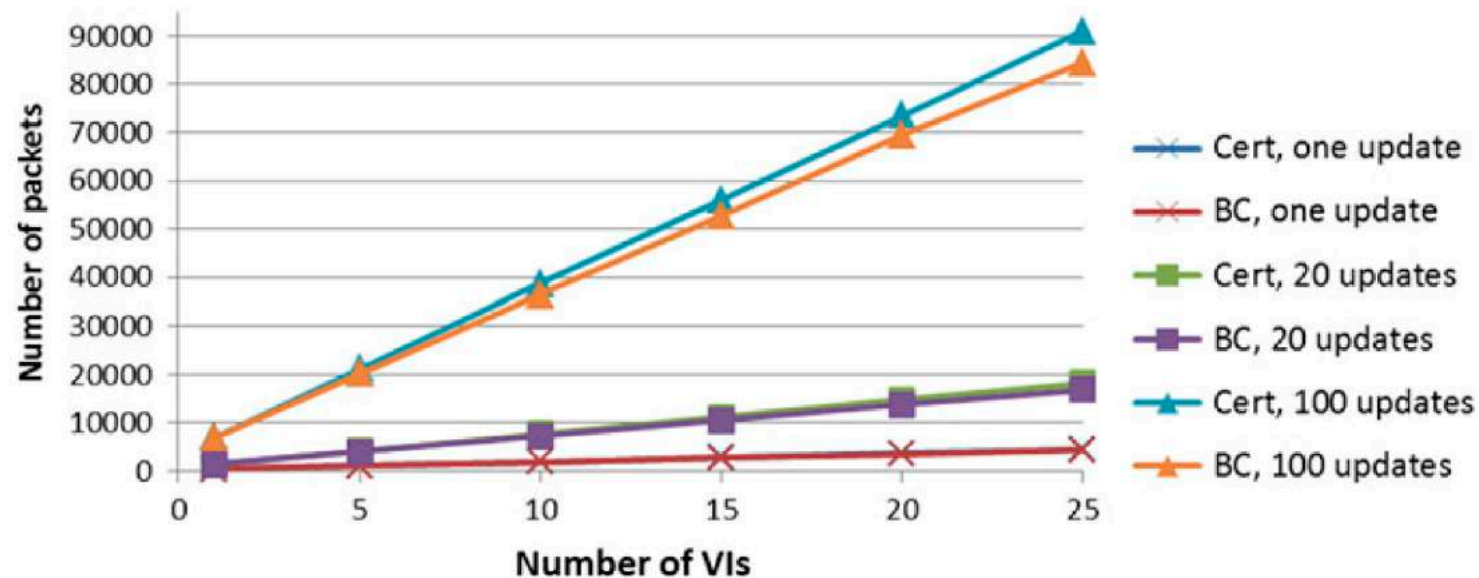


Fig. 4 **a** The WVI prototype based on a BeagleBone Black and our developed communication cape; **b** target ECU: Infineon AURIX ECU in the AURIX application kit TC277 TFT

Proof-of-Concept



Evaluation of the number of packets based on the number of Vehicle Interfaces (VI)

M. Steger et al. "BlockChains securing Wireless Automotive Software Updates – A proof of concept," Lecture Notes in Mobility (AMAA 2017) Berlin Germany, pages 137-149, August 2017.

Uber halts self-driving car tests after death

🕒 20 March 2018

f t m ✉ Share



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



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

Email

Twitter

Facebook

LinkedIn

Print

36

59

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

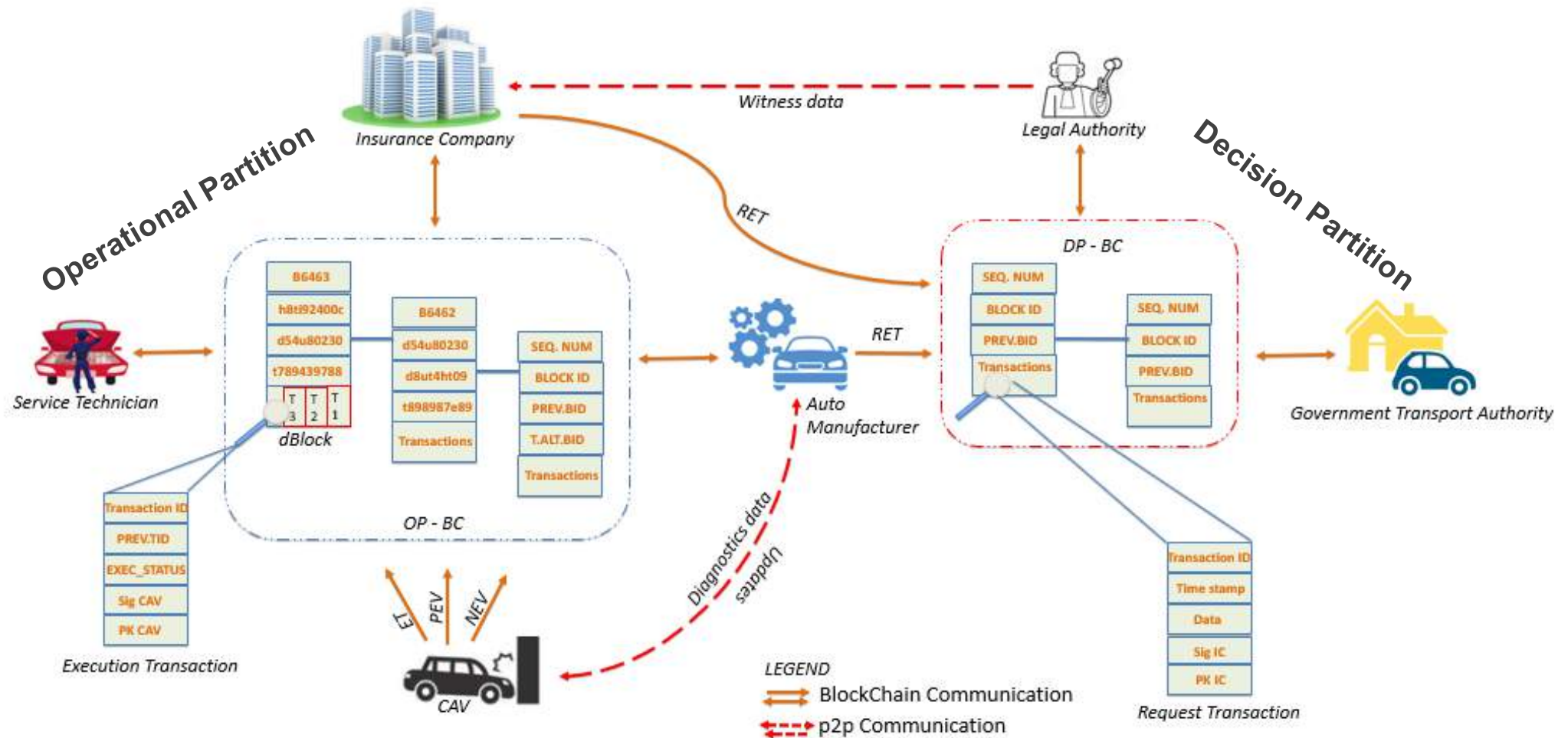


- Product Liability: blame is assigned to an auto manufacturer for product defect
- Service Liability: identified last action of a service technician caused the accident
- Negligence Liability: vehicle owner failed to adhere to instructions and is responsible

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, B-FICA: BlockChain based Framework for auto-Insurance Claim and Adjudication, in Proceedings of IEEE Blockchain, August 2018



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

B-FICA: Transaction verification



A transaction is successfully verified if

- Complete: has signatures of concerned entities.
- Authorization: transaction initiator is authorised to transact in either partitions.
- Unique: the transaction has not been previously received from same entity.

B-FICA: Transaction validation

In the OP-BC, given infrequent rate of transaction generation,

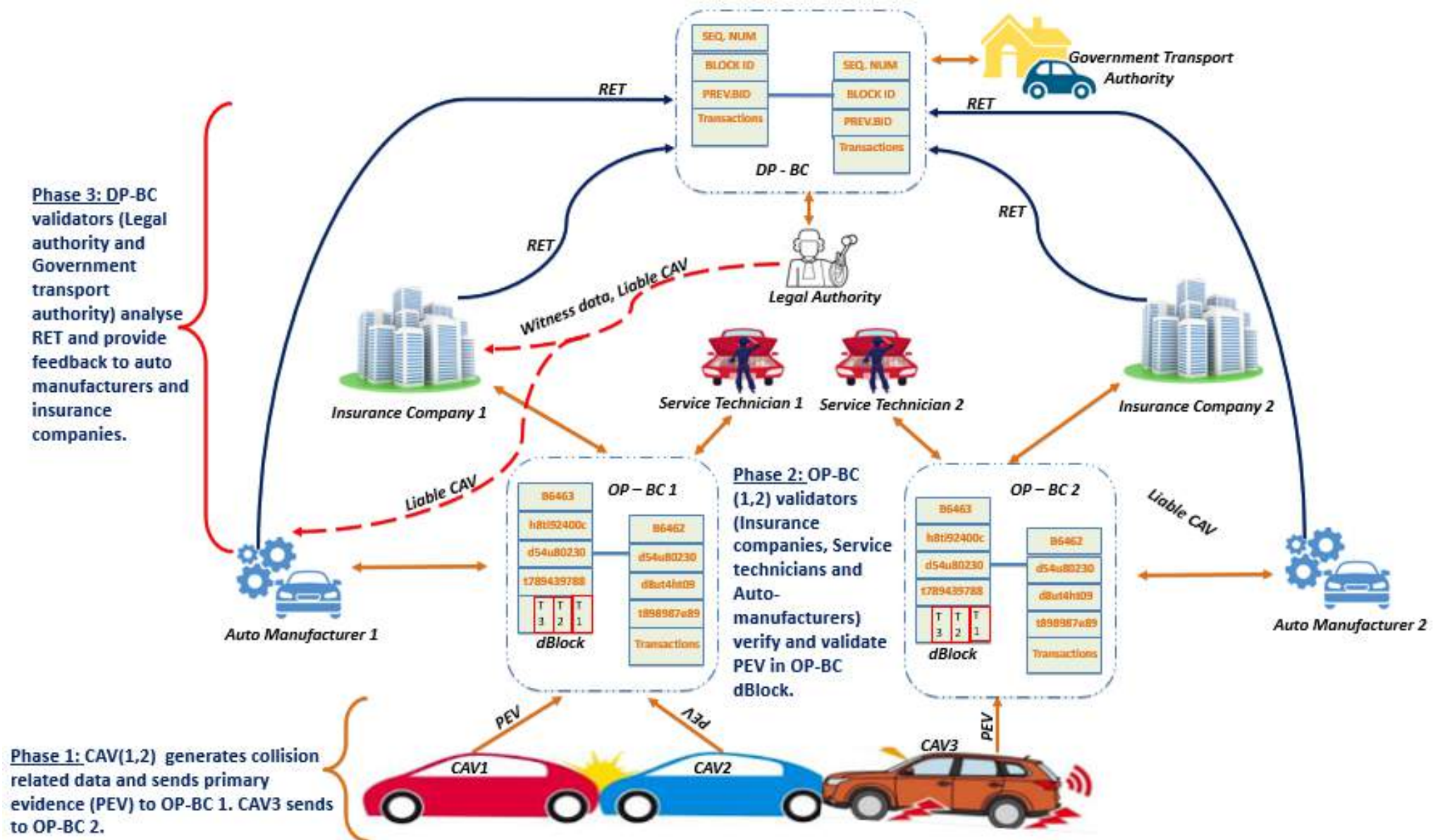
- Transactions are stored in a dynamic block;
- Dynamic block (dBlock) temporarily stores transactions until maximum allowance is reached.
- A dynamic light-weight consensus protocol is utilised to validate transactions.

```
For every successfully verified Transaction ;  
while  $dBlock < B_{Max}$  do  
     $ndB = Curr.T_{ID} + dBlock_{ID}$  ;  
end while
```

- This results in a new block identifier and used to secure transactions in the dynamic block.

In the decision partition, validation occurs when transactions reach maximum block allowance.

Illustrative Example: Three Car Collision



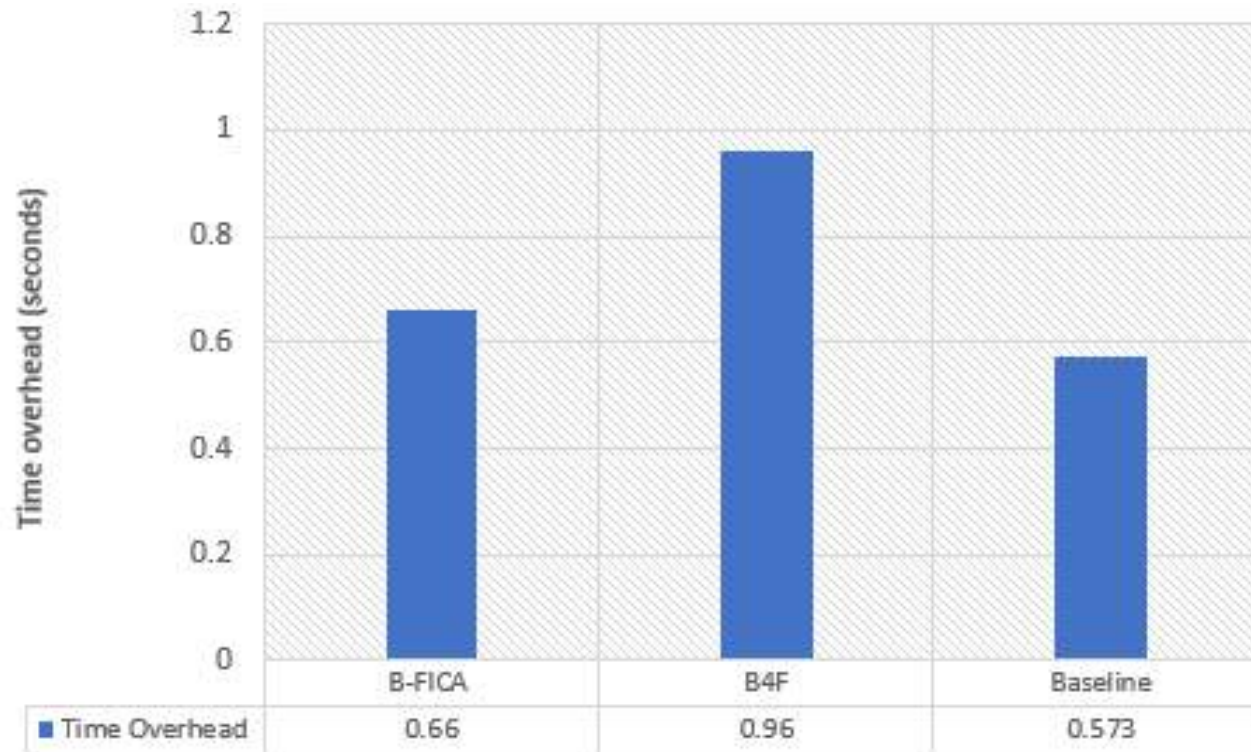
Security Analysis

Key requirement	Approach
Authorization	Partitions enable need-to-know communications. Verification credential unique for both partitions
Integrity	Transaction hash as identifier Data contents also hashed
Secure storage	Transaction validation in the dynamic block prevents evidence tampering and unavailability.
Non-repudiation	Transactions are signed by proposers and verified by validators to ensure auditability and prevent denial of actions.
Decentralization	No central source of trust. Collaborative data verification

Security Analysis: Attack model and defence

Attack model	Description	Defence mechanism
Transaction deletion	Rogue validator exploits the infrequent transaction generation rate to delete or alter evidence.	Dynamic block validation
False transaction	Rogue validators could collude to validate a false transaction to achieve same dynamic block state.	Consensus protocol (assuming validators cannot predict accidents)
Transaction modification	Vehicle manufacturer colludes with a vehicle owner to modify the contents of its accident-related data, computes a new hash, and sends a request transaction to decision partition validators.	Cross verification hash of transaction data of all proposers
Sensor alteration	A rogue validator could compromise an evidence generating sensor to produce authenticated messages with misleading information.	Validators cross verify data against every other data submitted by other CAVs in the scene of the event by checking time stamps and location information.

Performance Evaluation



M. Cebe, E. Erdin, K. Akkaya, H. Aksu and S. Uluagac, Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles.

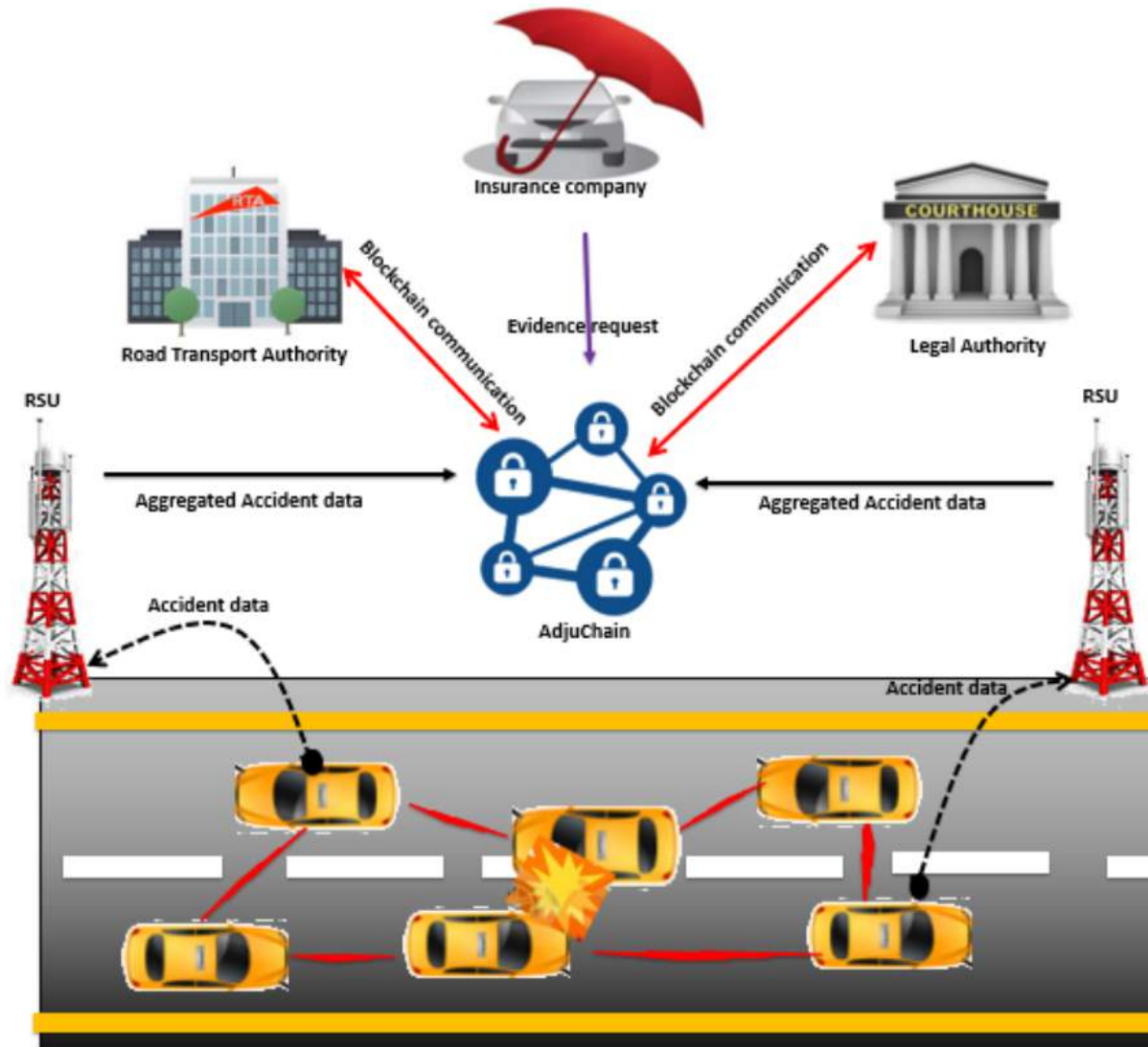
But do we trust the data?

The potential for remote exploitation for CAVs cast doubts on the reliability of data generated by the vehicle and utilised during forensic process for liability attribution.

The associated reputational and financial costs could motivate likely liable entities to execute rogue actions such as altering forensic data before or after storage or during data retrieval process to evade liability

Earlier works on data reliability in vehicular networks cannot be adapted for CAV forensics as they are both vulnerable to exploitation by likely liable entities and a single point of failure

Trust Management Framework



C. Oham, R. Jurdak, S. S. Kanhere, and S. Jha, "A Trust Management Framework for Vehicular Forensics", under review

Operational Tier

Vehicles in the event of an accident record their perception of the accident and forward their recorded data to roadside units (RUs) for trust evaluation

- Vehicles maintain a ring-buffer like storage where new data overwrites old ones
- In the event of an accident, telemetry and video data stored in the ring buffer contributes to evidence for adjudication
- RUs filter data based on the event type contained in data received from vehicles

RUs evaluates trust via a time and proximity verification algorithm to establish the presence of vehicles in event place at event time and then computes a credibility score for vehicles

RUs aggregate accident data and forward to the adjudication tier for final verification and credibility score approval

Adjudication Tier

Aggregated data received from RUs is verified by the road transport and legal authorities and stored for adjudication

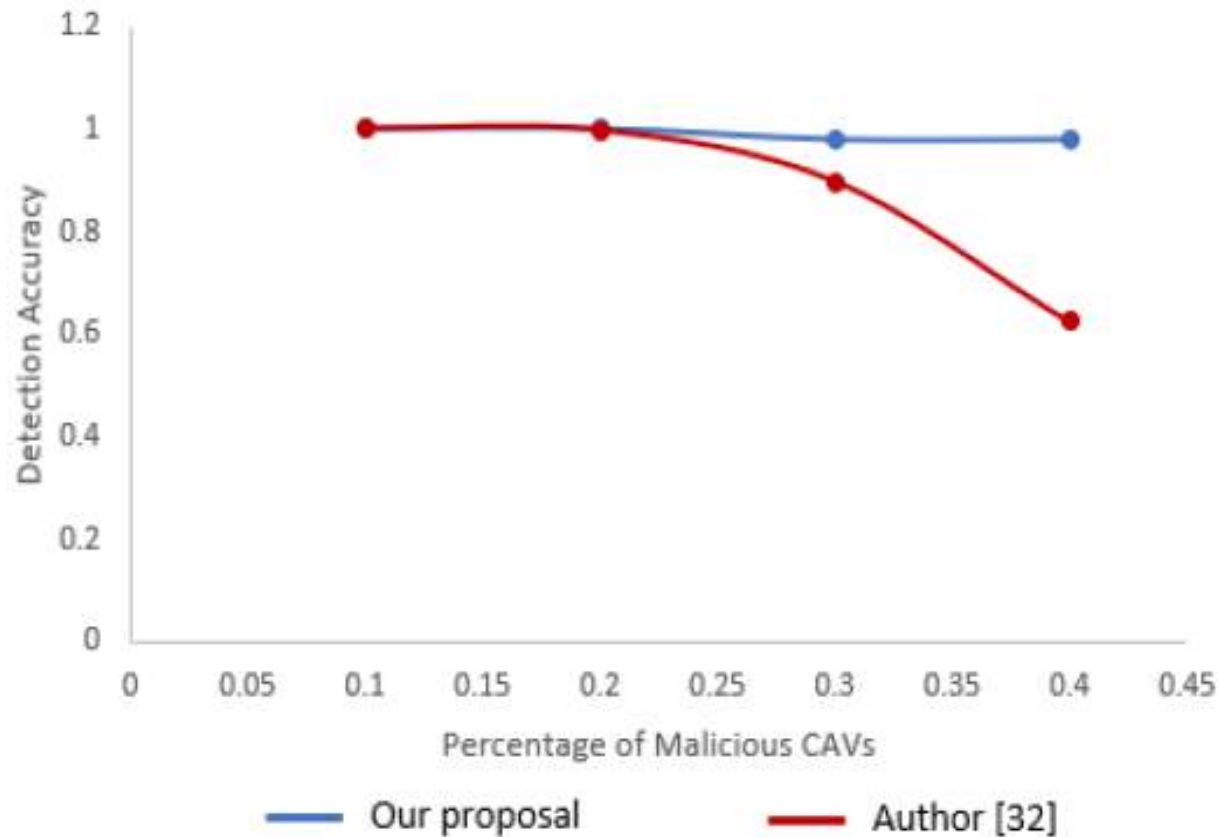
- This tier features AdjuChain; a blockchain platform where only successfully verified data are secured and utilized as contributing complimentary evidence for liability decisions.
- Entities here include the RUs, insurance companies, legal and transport authorities
- To prevent unauthorised access to sensitive data, legal and road transport authorities acts as validators and are responsible for the verification and validation of the data

As final verification for data credibility, validators correlate computed credibility score with data telemetry and video data and approve computed scores where verification is successful

Validators pack successfully verified data into a block (CredBlock), compute the hash of the block and append it to AdjuChain

Upon request, validators present reliable complimentary evidence to insurance companies or forensic analysts for expediting liability decisions

Performance Evaluation









[32] Z. Yang, K. Zheng, K. Yang and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Montreal, QC, 2017, pp. 1-5. doi:10.1109/PIMRC.2017.8292724

4

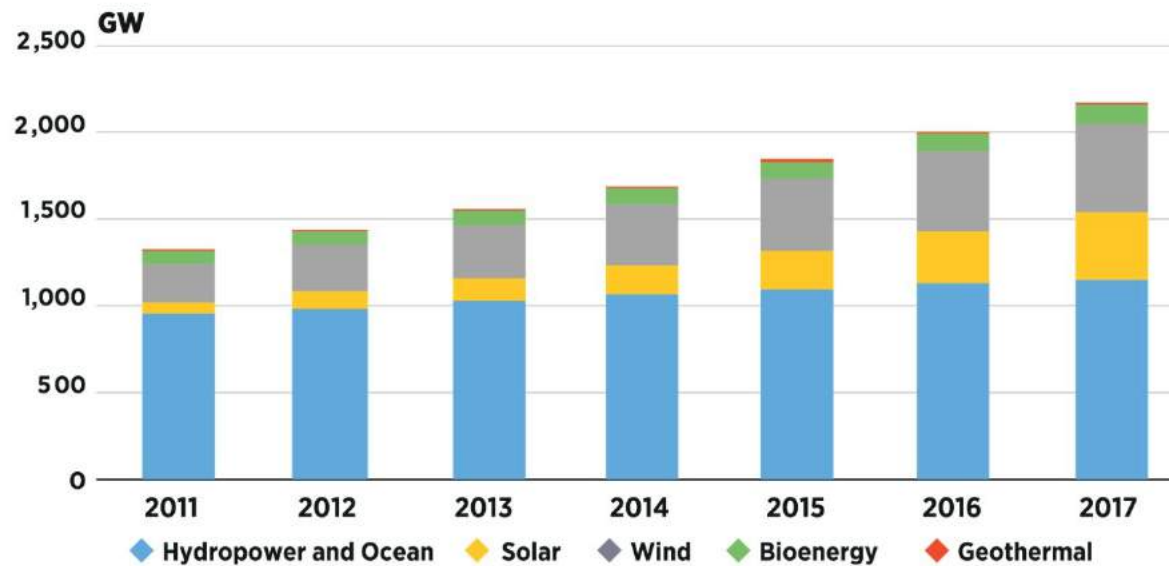
ENERGY TRADING



Renewable Energy Sources

					
Solar	Wind	Geo	Hydro	Bio	Tide

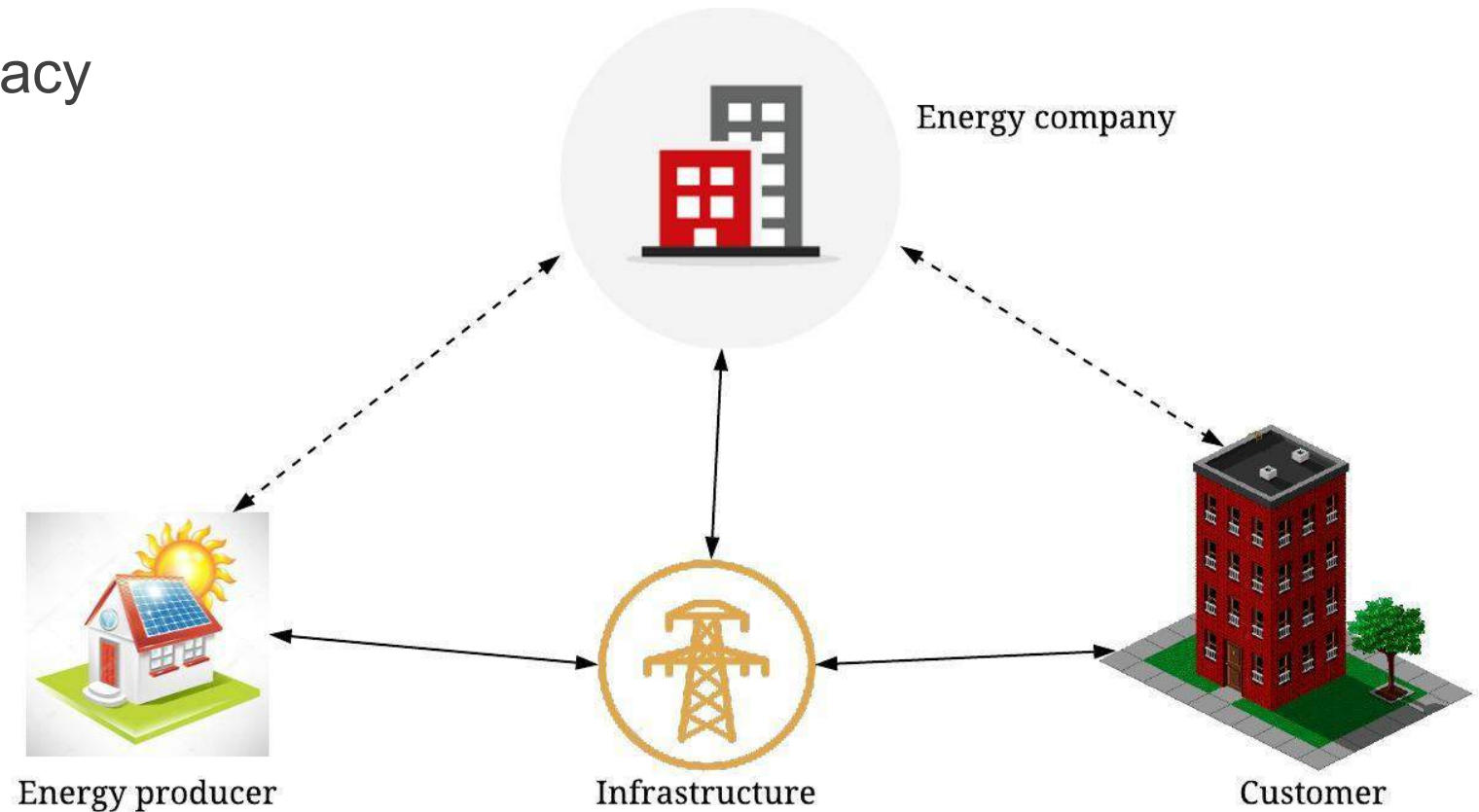
Total Renewable Power Generation Capacity, 2011-2017



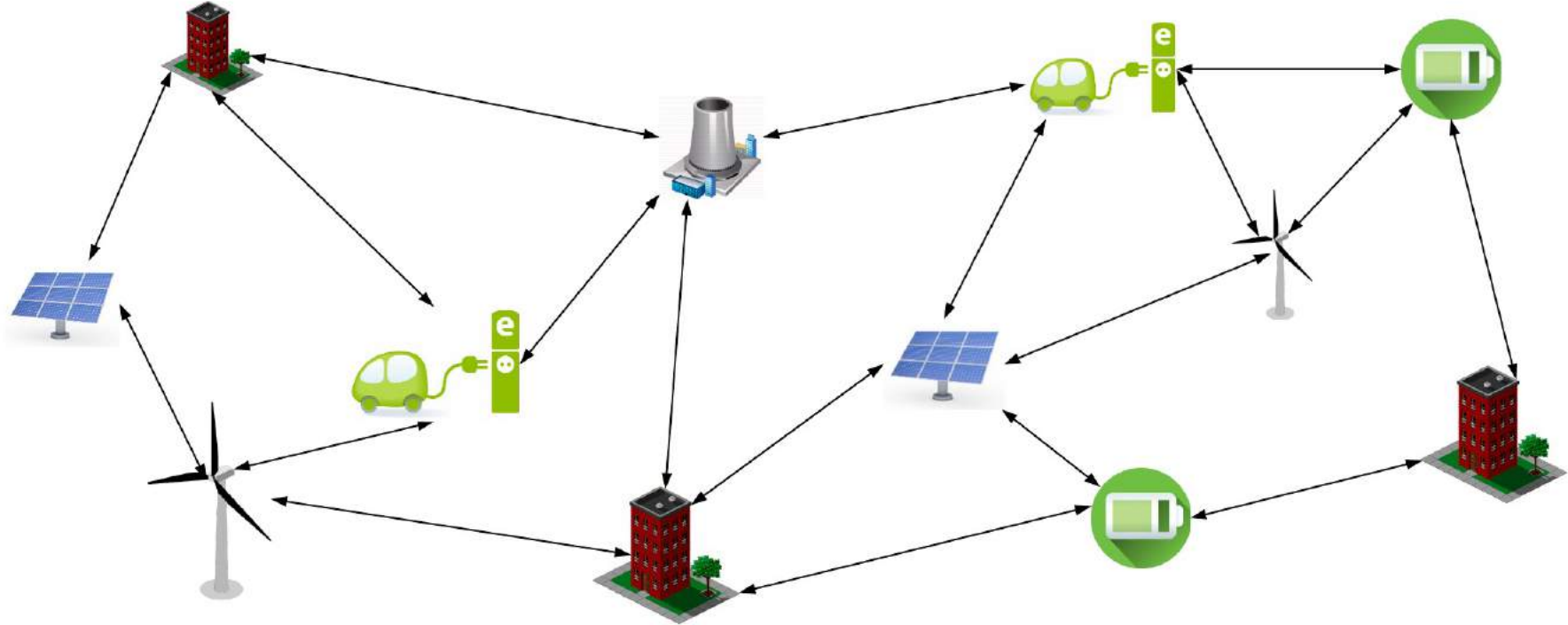
Conventional Energy Trading

Challenges

- Centralization
- Lack of Privacy

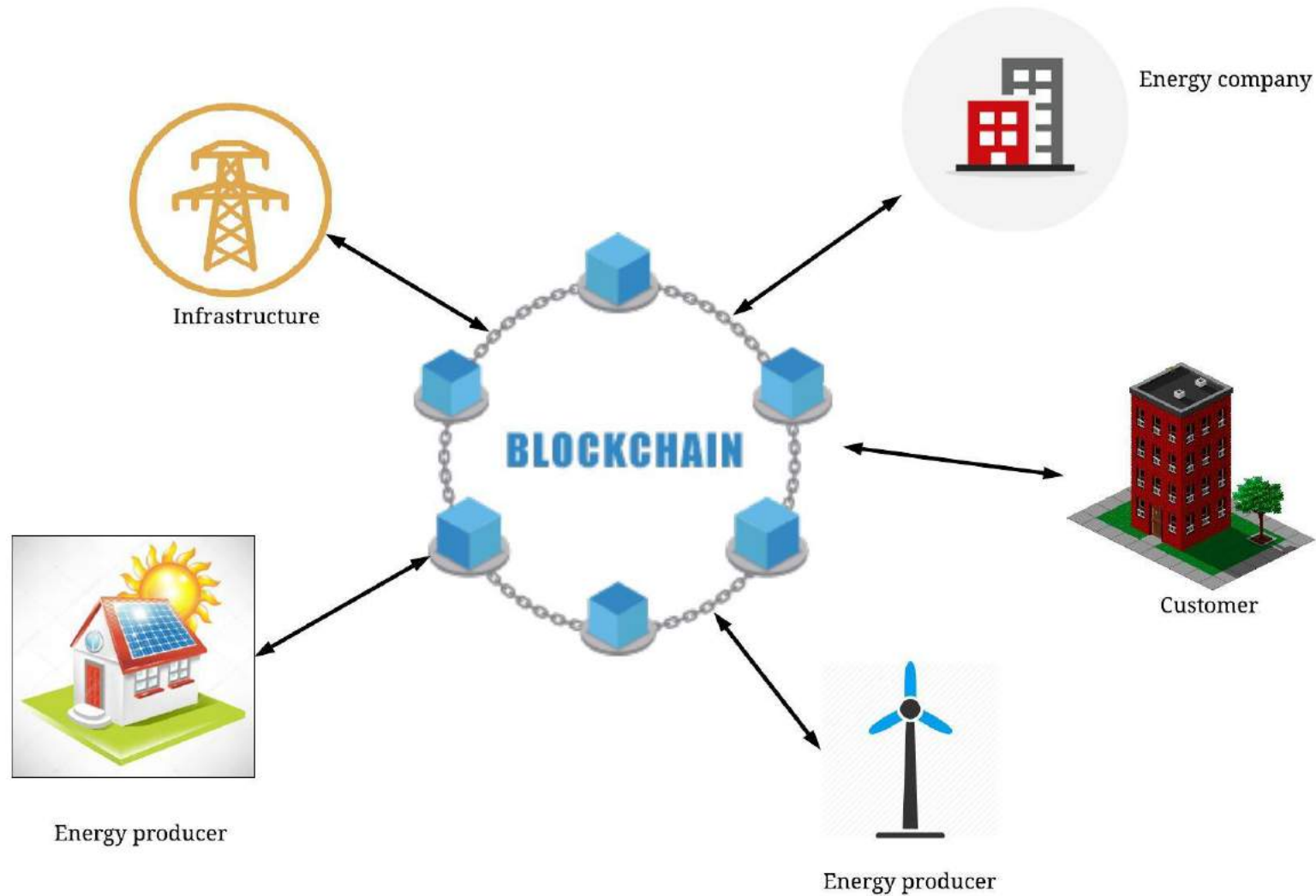


Peer to Peer Energy Trading



Increased integration of distributed energy resources
Traditional Consumers -> Prosumers

Blockchain-based Energy Trading



Challenges

- Lack of Privacy
 - Malicious nodes can monitor the pattern of transactions generated by a node, thus compromise the user privacy
- Relying on TTP
 - Most of existing methods rely on a third party to ensure both sides in energy trading fulfil their commitments
- Blockchain overheads
 - Negotiation messages are generally broadcast to all participants

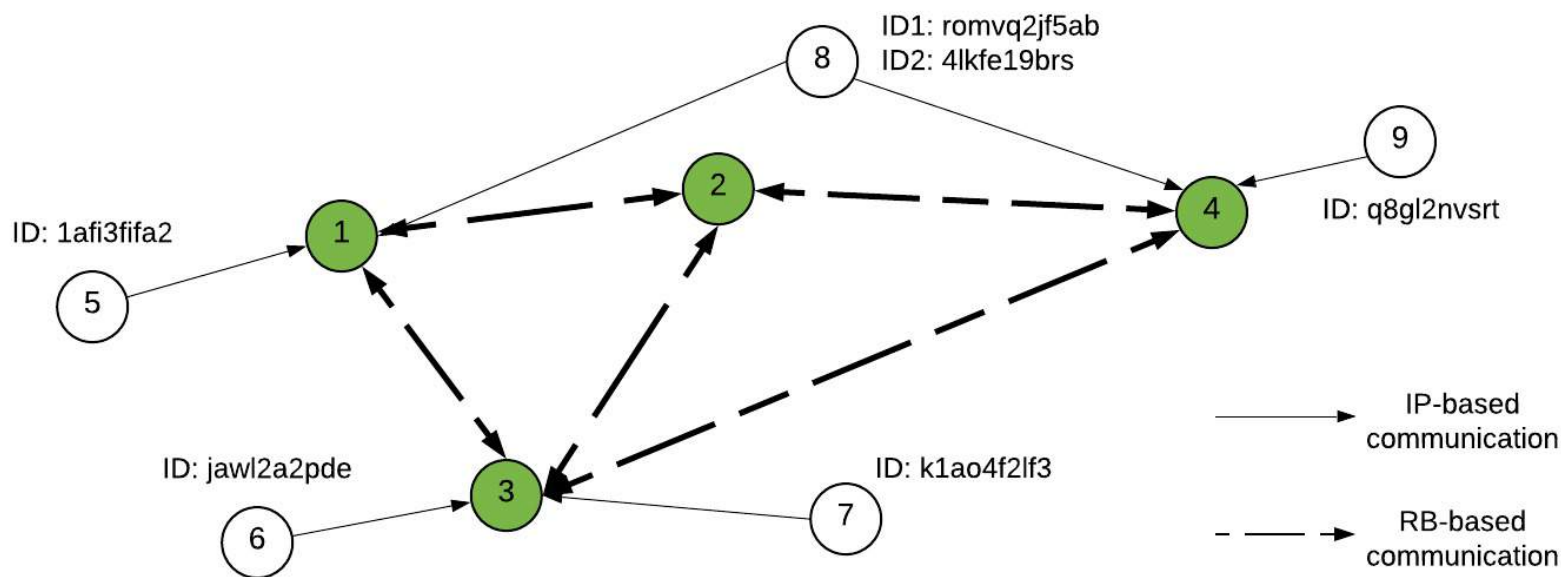
Secure Private Blockchain-based (SPB) Energy Trading

- An anonymous routing method on top of the blockchain
- A purely distributed trading method by introducing atomic meta-transactions
- A private authentication method to verify smart meters

A. Dorri, F. Luo, S.S. Kanhere, R. Jurdak and ZY Dong, SPB: A Secure Private Blockchain-based Solution for Energy Trading, IEEE Communications Magazine, in press.

SPB: Routing (Anonymous Routing Backbone)

- PK based routing algorithm
- High resource available devices form a backbone network and route packets
- Backbone nodes uses conventional routing methods to route packets



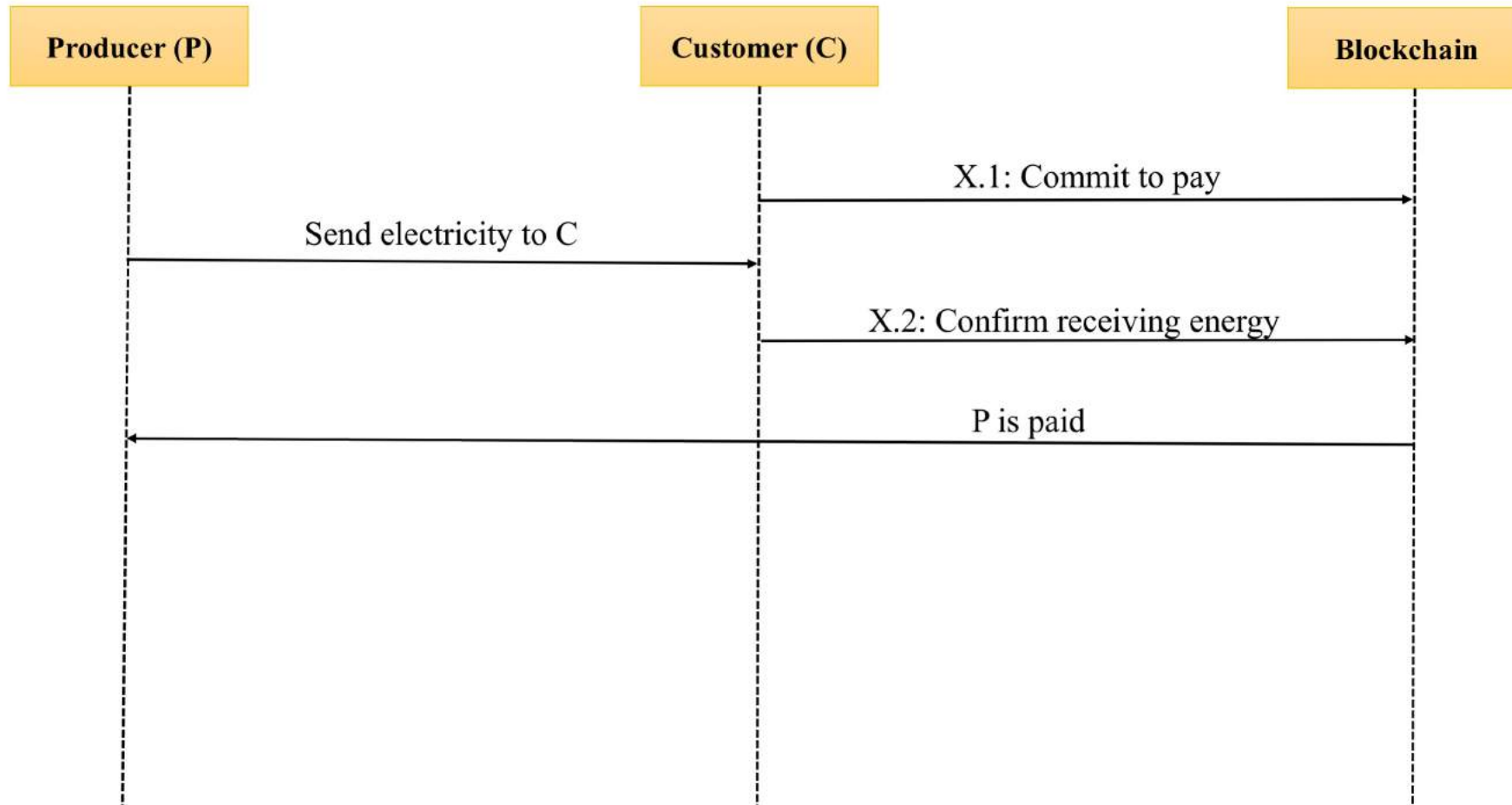
Distributed Hash Table

Node	Keys
1	0-9
2	a-f
3	g-l
4	m-z

SPB: Transactions

- Atomic meta-transactions
 - An atomic meta-transaction is valid only if two transactions are generated within a specific time period
 - Incomplete transactions will be removed after the time period
- Consists of two transactions
 - Commit to Pay (CTP):
 - Generated by the consumer to commit payment of the energy price
 - Money is not transferred to the producer account
 - Not stored in blockchain, stored in a CTP database
 - Energy Receipt Confirmation (ERC):
 - Generated by the smart meter of the consumer to confirm receipt of energy
 - Assume that meters are tamper resistance

SPB: Energy Trading Process



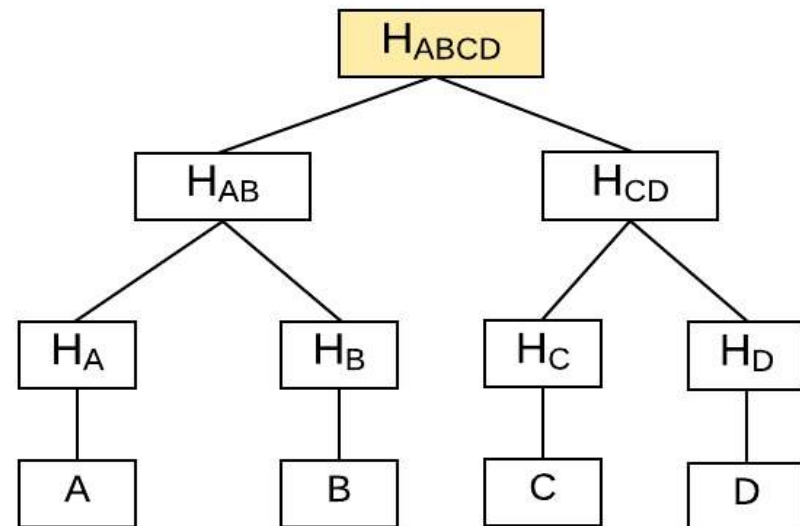
SPB: Issues

- The participating nodes need to ensure that the ERC is signed by a genuine smart meter
- The ERC transaction generated by the smart meter reveals information about the energy consumption/production of the user



SPB: Certificate of Existence (COE)

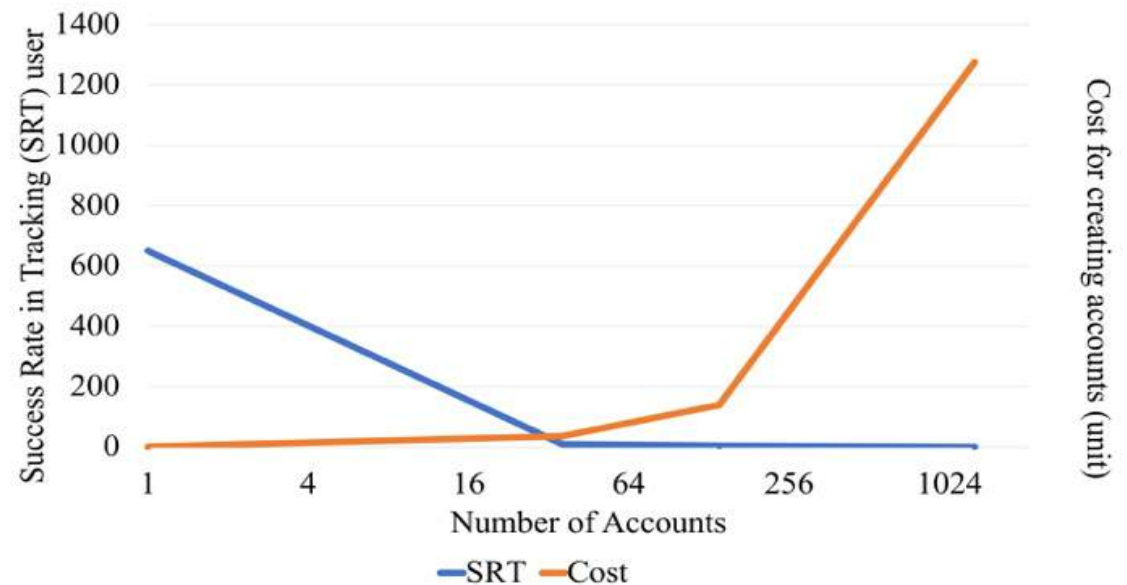
- Meter manufacturer assigns a unique public/private key pair to each meter and serves as CA for those keys
- Each meter creates a number of keys and forms a Merkle tree of the PKs
- The meter sends the root hash of the Merkle tree to another meter to be signed
- Signed root to be used as COE

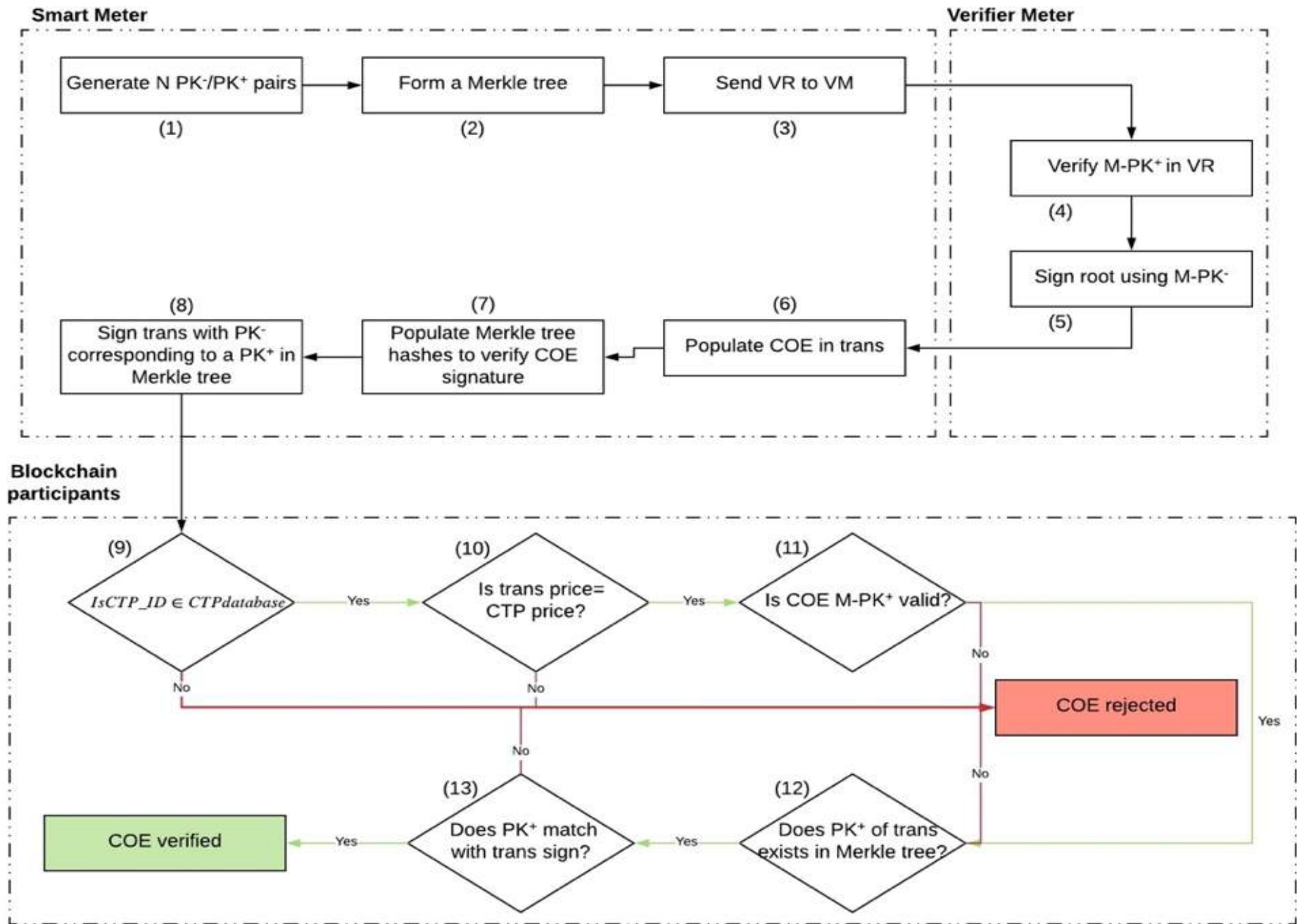


SPB: Certificate of Existence (COE)

- To protect privacy, a single COE may be used by more than one meter
- The meter that signs the COE is chosen randomly, even the meter itself might sign the COE
- The anonymity level of the user depends on the number of accounts he employed to store his transactions

Han, Seungyeop, et al. "Expressive privacy control with pseudonyms." ACM SIGCOMM Computer Communication Review. Vol. 43. No. 4. ACM, 2013.

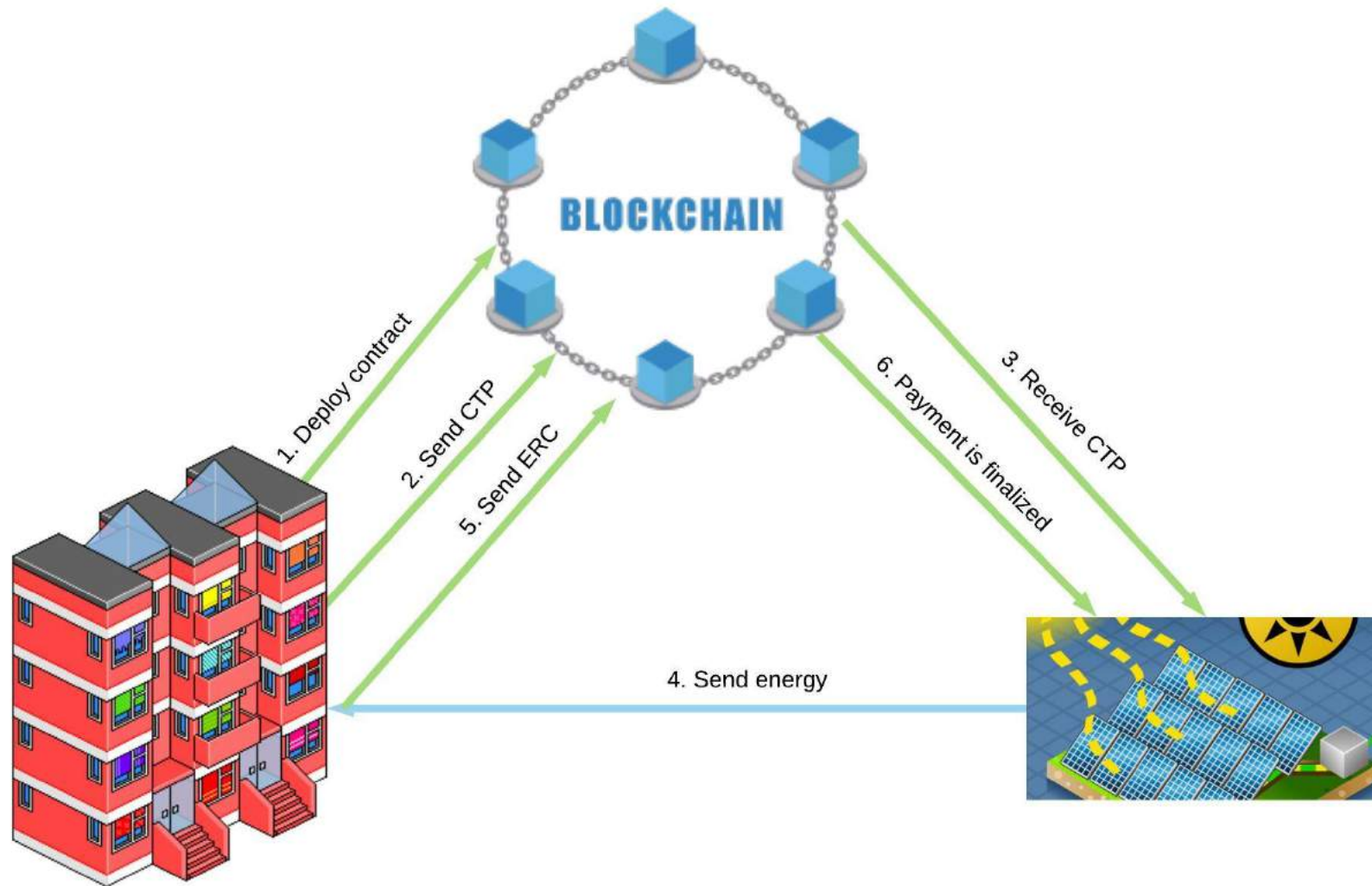




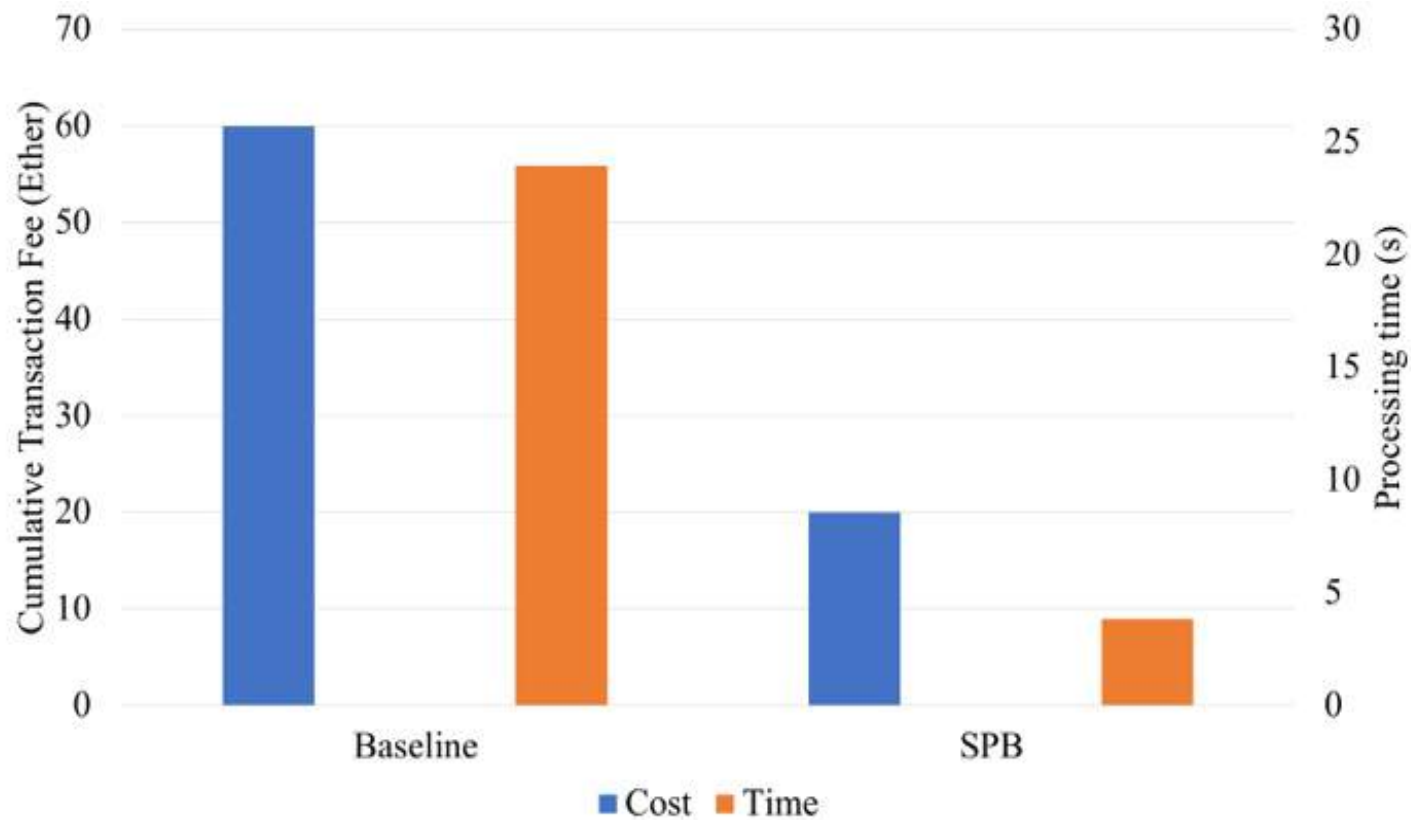
Performance Evaluation

- We have implemented SPB in Ethereum testnet
- Smart contract is deployed using Solidity
- Three nodes participate in network, energy consumer, producer and miner
- Online demo available at:
https://www.youtube.com/watch?v=rX58GO_hQqI

Performance Evaluation



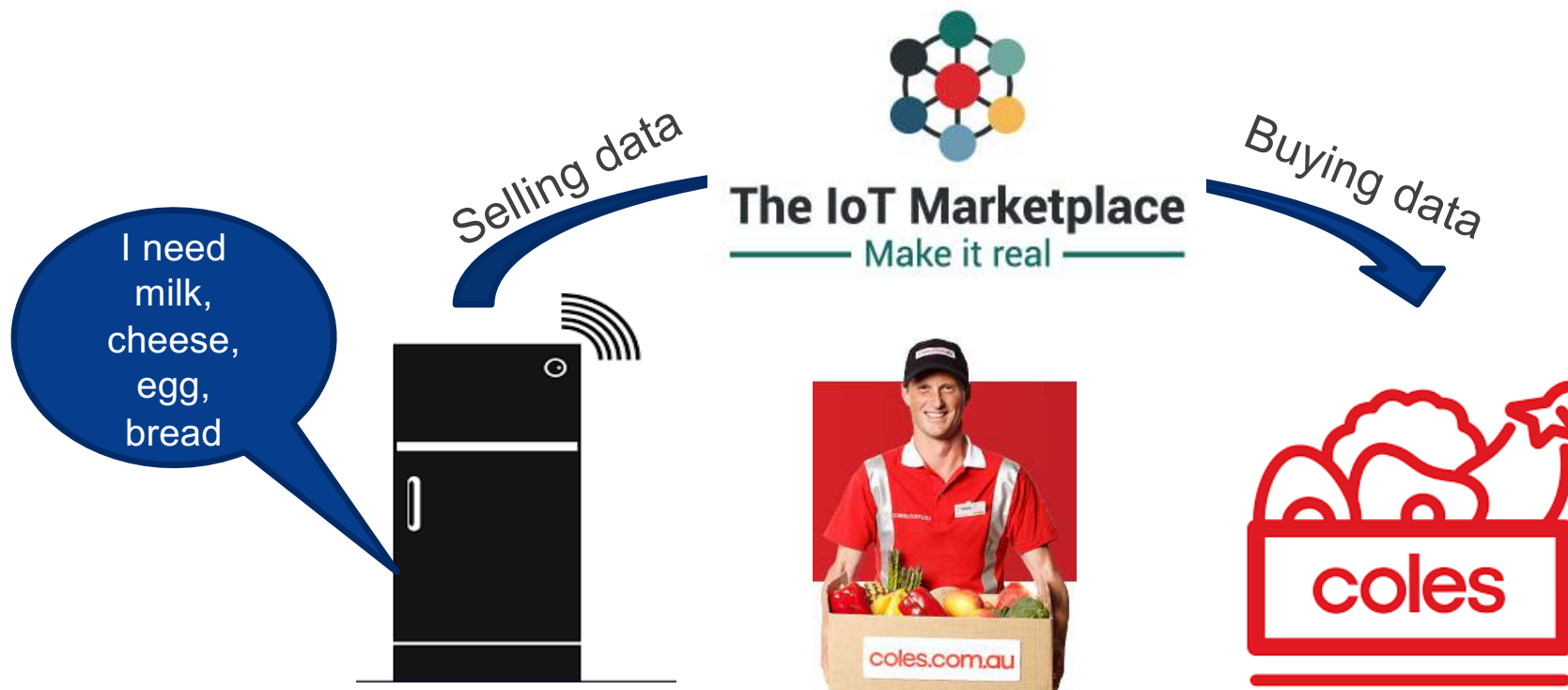
Performance Evaluation



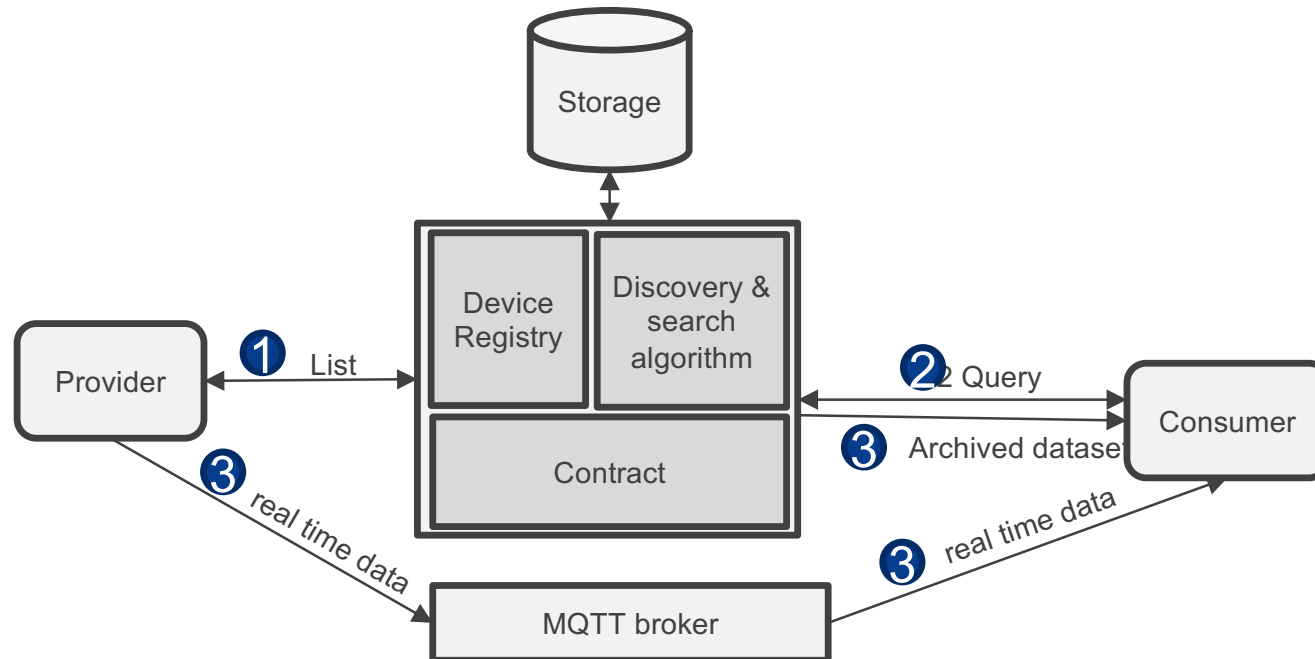
Future Directions

- Evaluating the concept using extensive implementations
- Applying the concept in smart grid
- Extending the work for smart grid energy load balancing

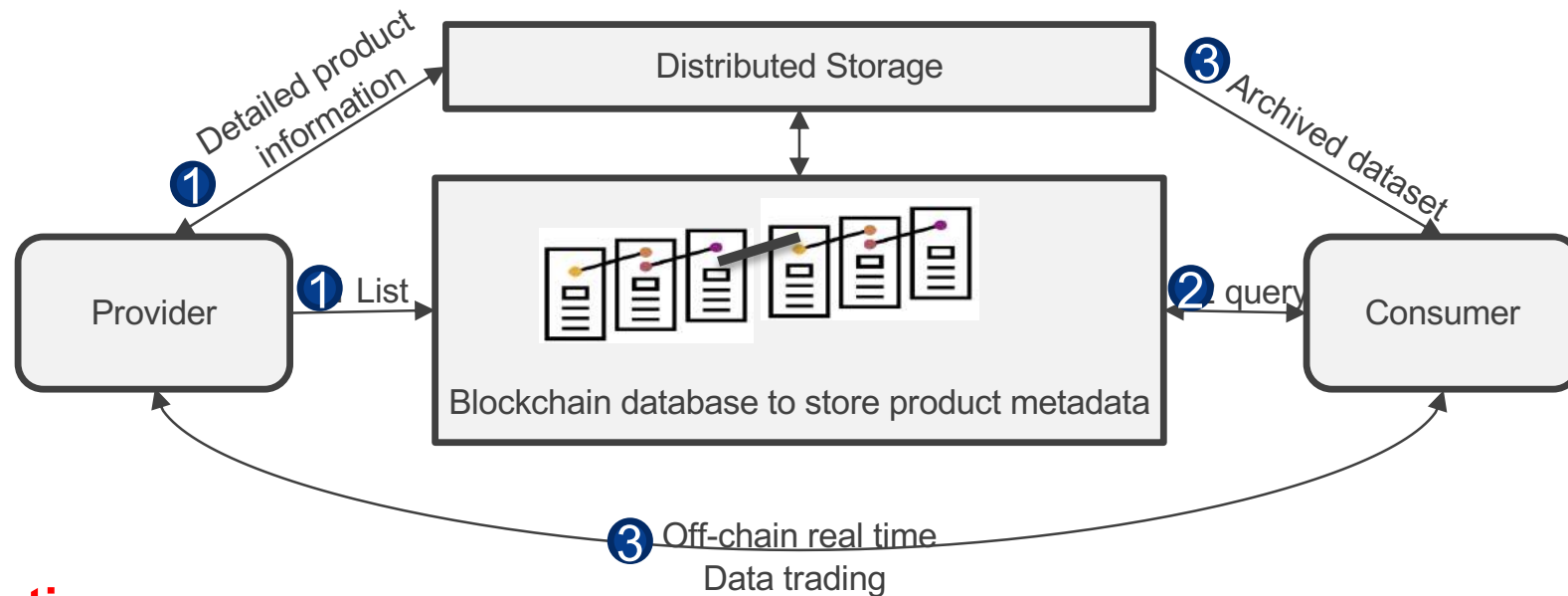
**WE'VE
GOT
ISSUES**



State-of-the-art : Centralized IoT Marketplaces



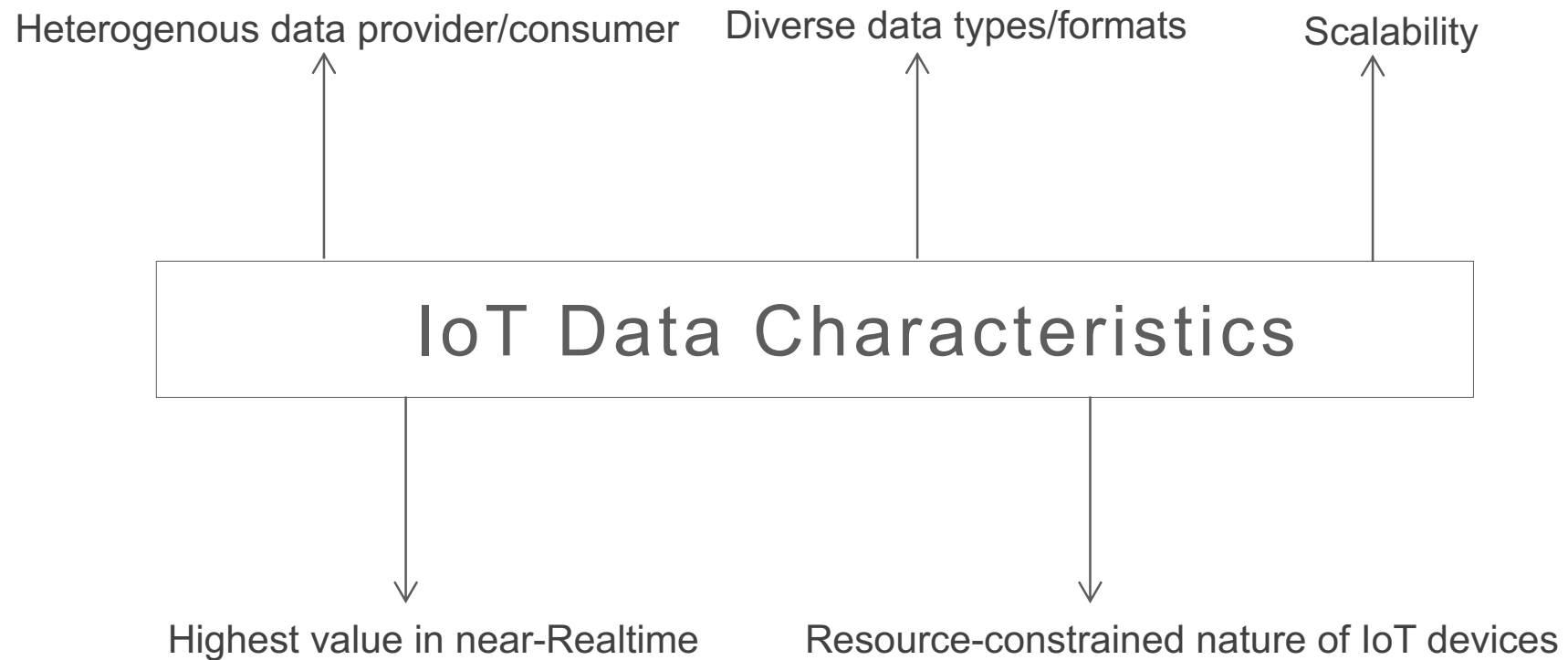
State-of-the-art : BC-based IoT Marketplaces



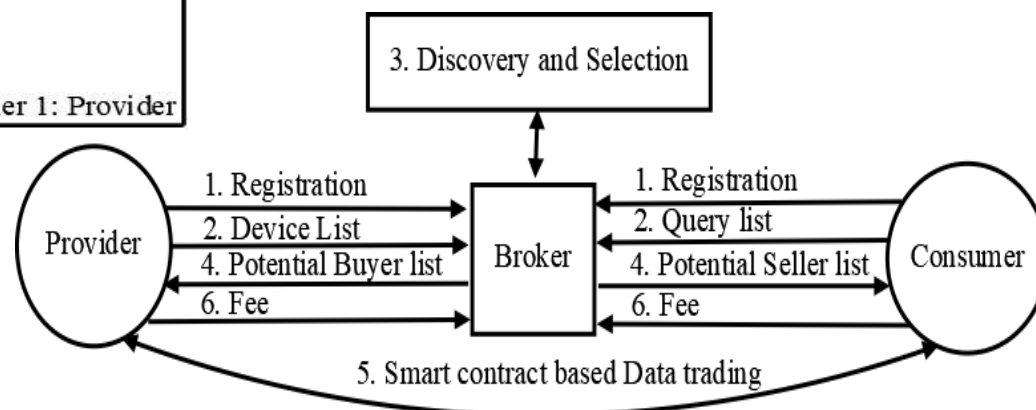
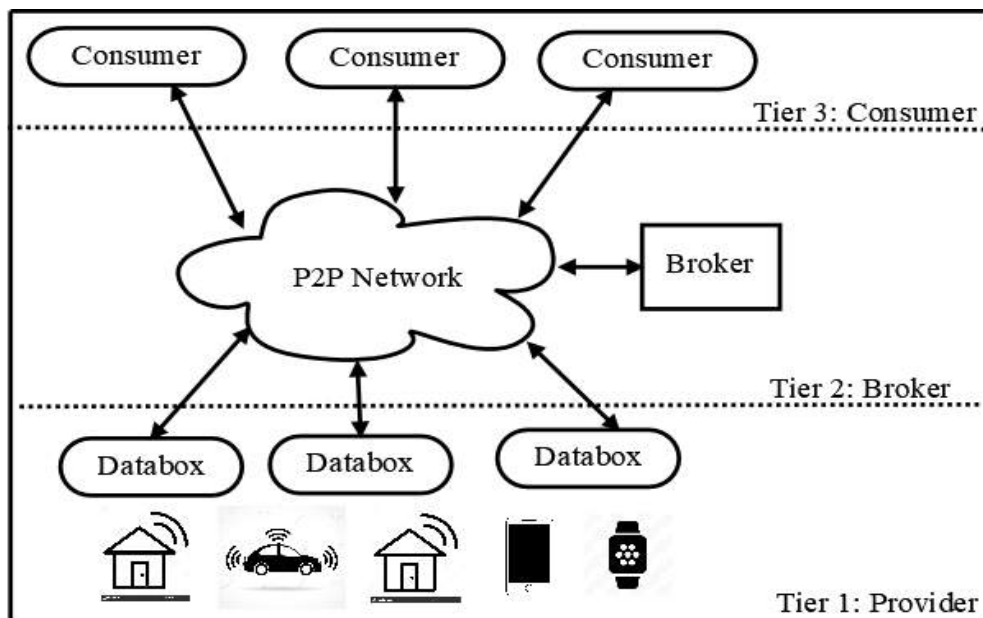
Limitations:

- Blockchain is used as a database for storing product information while the computation capability of smart contract is wasted
- Works only for small-scale and design gets fragmented with device mobility

Specific Framework for IoT device's data

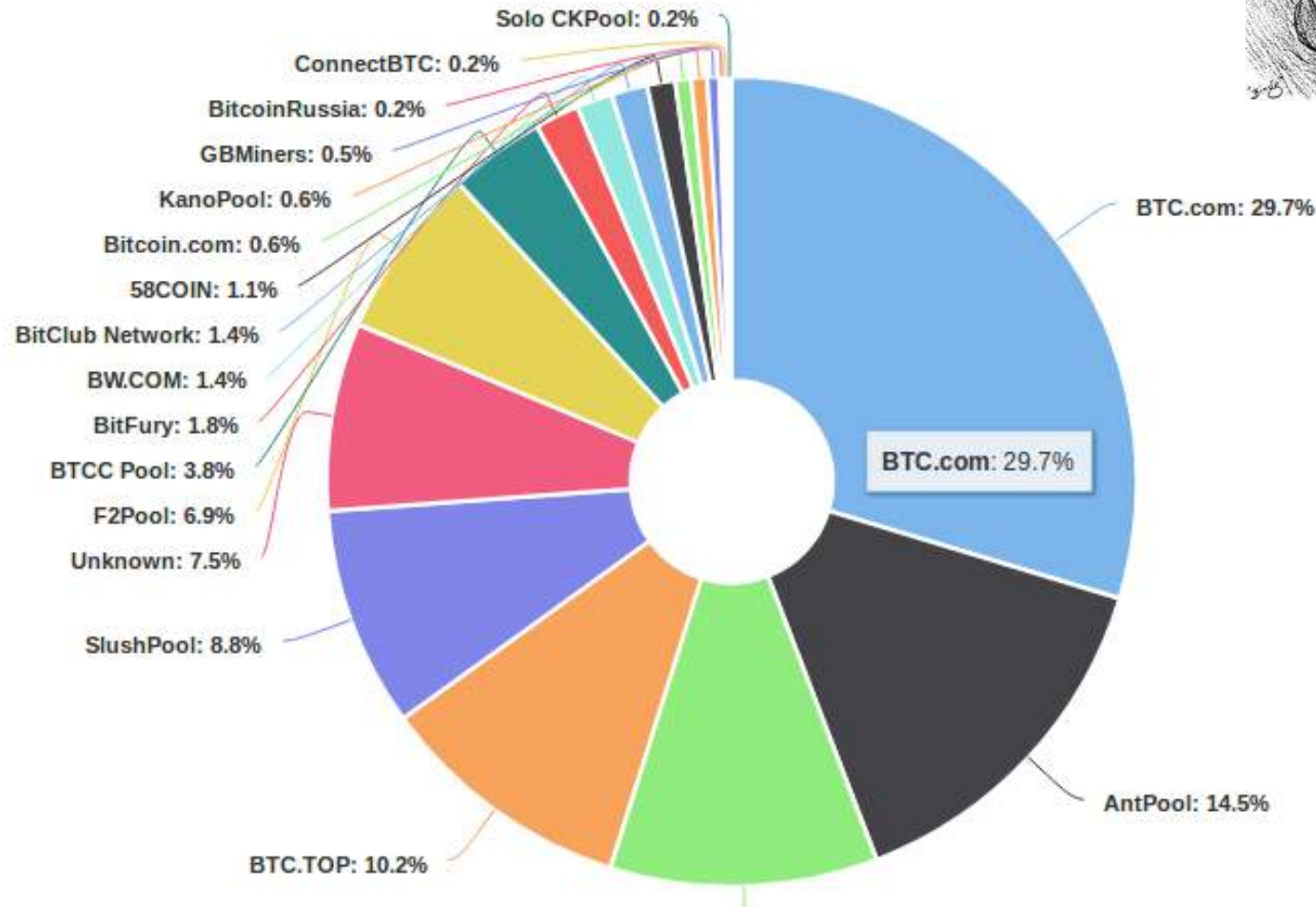


A Decentralized IoT Marketplace



P. Gupta, S.S. Kanhere, R. Jurdak, A Decentralized IoT Data Marketplace, In proceedings of the 3rd Symposium on Distributed Ledger Technology, Gold Coast, Australia, November 2018.

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

What about performance?



BLOCKBENCH: A Framework for Analyzing Private Blockchains

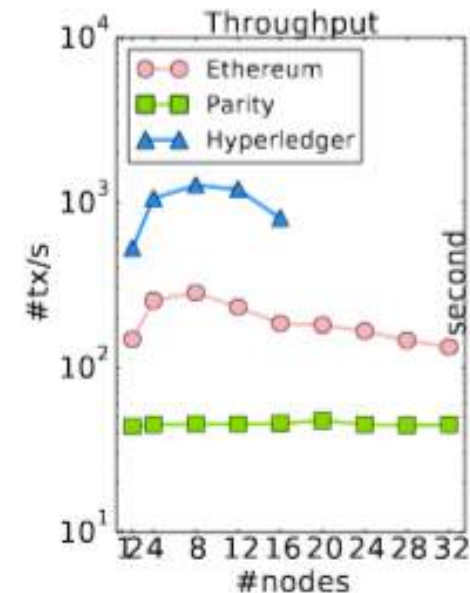
Tien Tuan Anh Dinh[‡] Ji Wang[‡] Gang Chen[§] Rui Liu[‡] Beng Chin Ooi[‡] Kian-Lee Tan[‡]

[‡] National University of Singapore [§] Zhejiang University

[‡] {dinhtta, wangji, liur, ooibc, tankl}@comp.nus.edu.sg [§] cg@zju.edu.cn



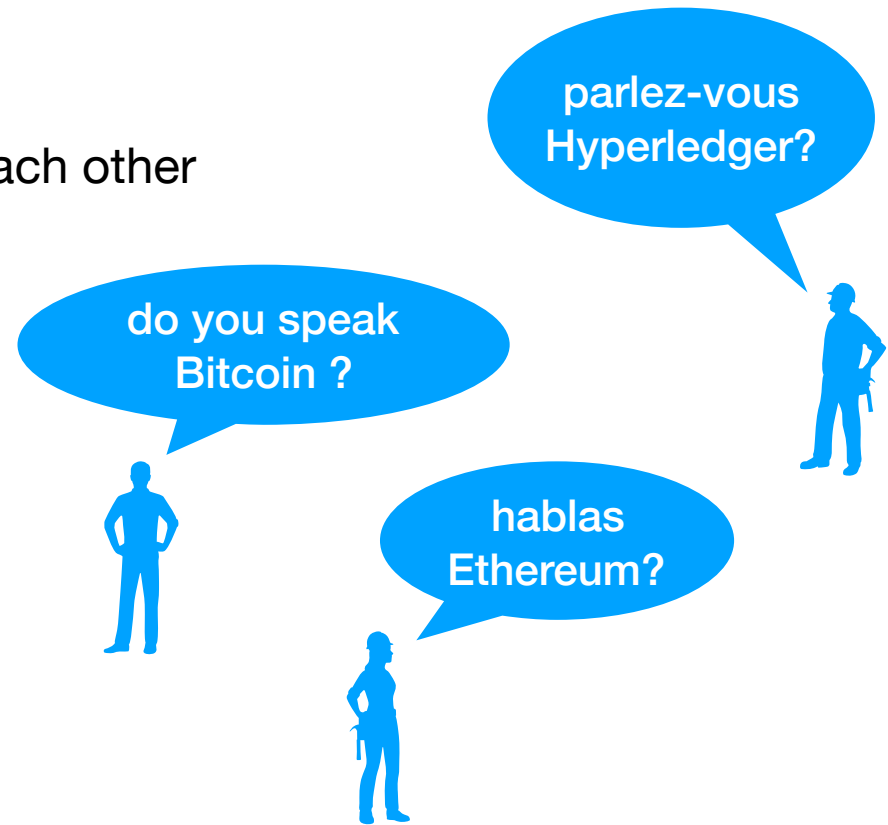
Figure 3: Abstraction layers in blockchain, and the corresponding workloads in BLOCKBENCH.



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

Challenges

- Interoperability
 - platforms should be able to talk to each other
 - incompatible Blockchain platforms
 - lack of standards



Internet of Blockchains

Blockchain of Blockchains

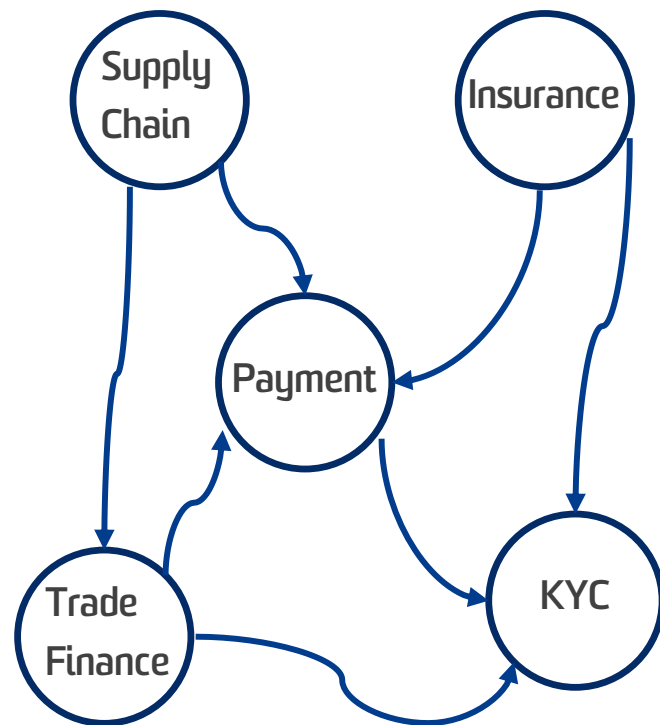
Cross chain communications

Multi-chains

Relay Chains



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



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!!!



W: www.research.csiro.au/dss,
www.jurdak.com
E: raja.jurdak@csiro.au

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



- [1] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and Solutions." arXiv preprint arXiv:1608.05187 (2016).
- [2] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized BlockChain for IoT", Second IEEE/ACM International Conference on Internet-of-Things Design and Implementation (IoTDI) 2017
- [3] A. Dorri, S. S. Kanhere, and R. Jurdak, and P. Gauravaram. "Blockchain for IoT security and privacy: The case study of a smart home." In *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*, pp. 618-623. IEEE, 2017.
- [4] A. Dorri, S. S. Kanhere, and R. Jurdak, and P. Gauravaram, "A Lightweight Scalable Blockchain for IoT", under review.
- [5] A. Dorri, M. Stegar, S. S. Kanhere, and R. Jurdak, "Blockchain: A Distributed Solution to Automotive Security and Privacy", in IEEE Communications Magazine, December 2017
- [6] M. Steger, A. Dorri, S. S. Kanhere, K. Roemer, R. Jurdak and M. Karner, "Secure Wireless Automotive Software Updates Using Blockchain: A Proof-of-Concept" in Proceedings of Advanced Microsystems for Automotive Applications, 2017
- [7] S. Malik, S. Kanhere, R. Jurdak, "ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains," In proceedings of IEEE International Symposium on Network Computing and Applications (NCA), Cambridge, USA, November, 2018.
- [8] C. Oham, R. Jurdak, S. Kanhere, A. Dorri, S. Jha, "B-FICA: BlockChain based Framework for auto-Insurance Claim and Adjudication," In proceedings of The IEEE International Conference on Blockchain (Blockchain 2018), Halifax, Canada, July, 2018.
- [9] P. Gupta, S.S. Kanhere, R. Jurdak, A Decentralized IoT Data Marketplace, In proceedings of the 3rd Symposium on Distributed Ledger Technology, Gold Coast, Australia, November 2018.
- [10] A. Dorri, S.S. Kanhere, R. Jurdak, A Memory Optimized and Flexible BlockChain for Large Scale Networks, Future Generation Computer Systems, October, 2018. Volume 92, Pages 357-373, March 2019.

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

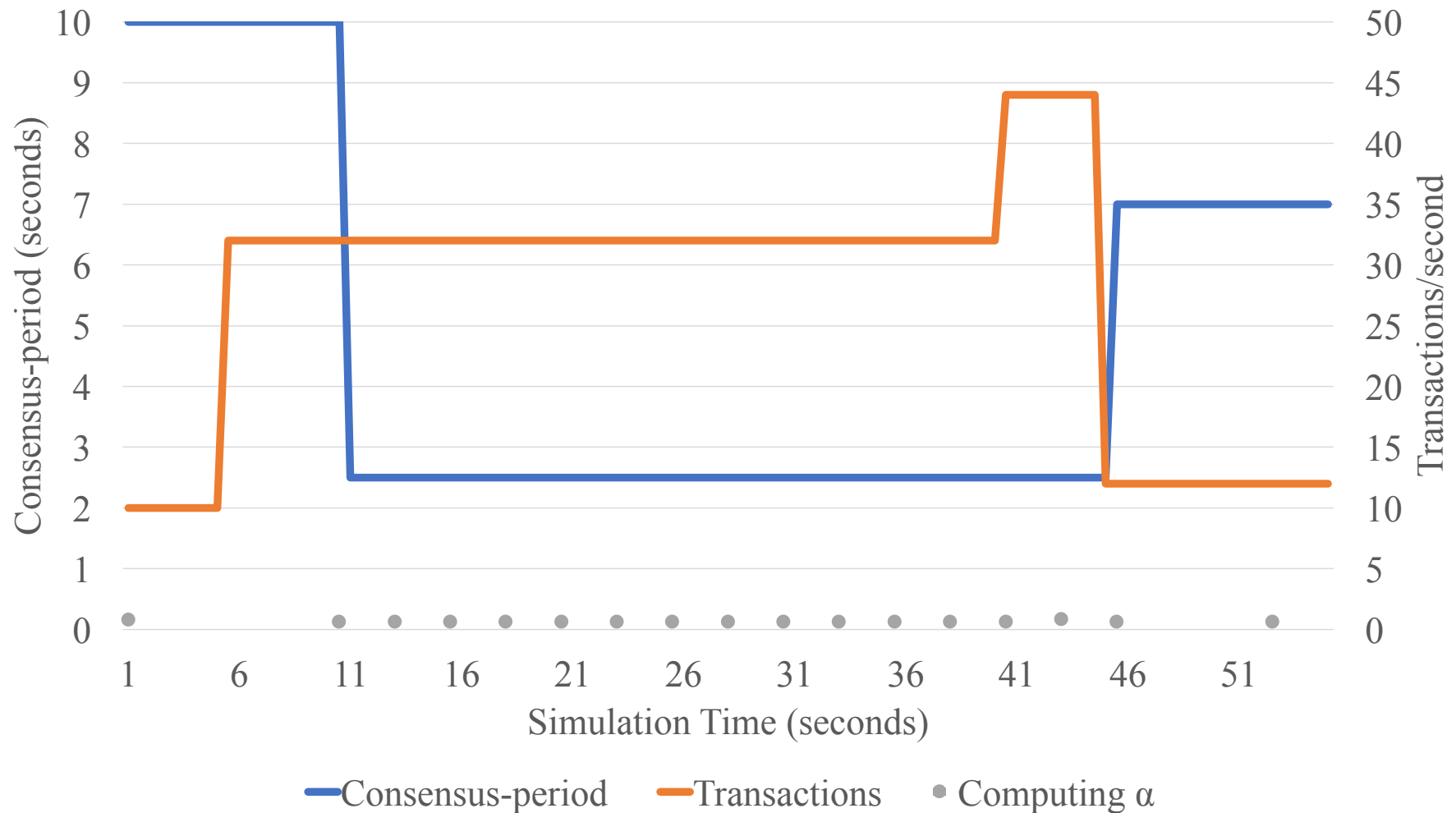
- if the requestee is not part of the OBMs cluster, then the transaction is broadcast to other OBMs

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

Distributed Throughput Management





Discussion

Auditability

- All transaction records are permanently stored
- Records can be used for audits, criminal investigations, etc.

Incentives for OBMs

- Implicit rewards in the form of reputation
- Advertising for service/cloud providers

MOF-BC: Initiating Memory Optimization



Optimization can be done by:

- User Initiated Memory Optimization (UIMO)
 - The end user initiates the transaction removal once generating the transaction
- SP Initiated Memory Optimization (SIMO)
 - The SP initiates the transaction removal once generating the transaction
- Network Initiated Memory Optimization (NIMO)
 - The end user authorizes the network to handle the removal of the transaction once particular situation is met

UIMO and SIMO transaction removal



- Each user must store the keys corresponding to the transaction to prove ownership of the transaction and thus remove
- User ends up with millions of keys
- MOF-BC introduces *generator verifier (GV)* to address key management
 - All transactions are managed using a single key that can be biometric information of the user
 - Protects the privacy of the user as GV is different even if the same GVS is applied

$$GV = GV-PK (P_T_ID \parallel GVS)$$

NIMO transaction removal



- New fields are added to transactions:

MOM || MOM-Setup

- Agents manage the transaction based on the optimization mode
- Secure: Hash of the transaction is signed by the user

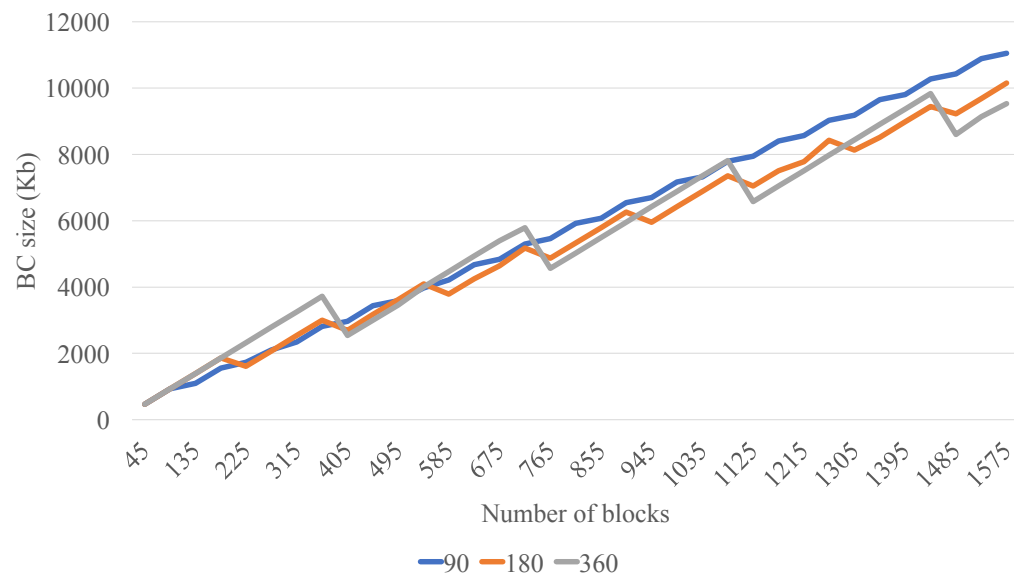
Performance Evaluation

Table 4

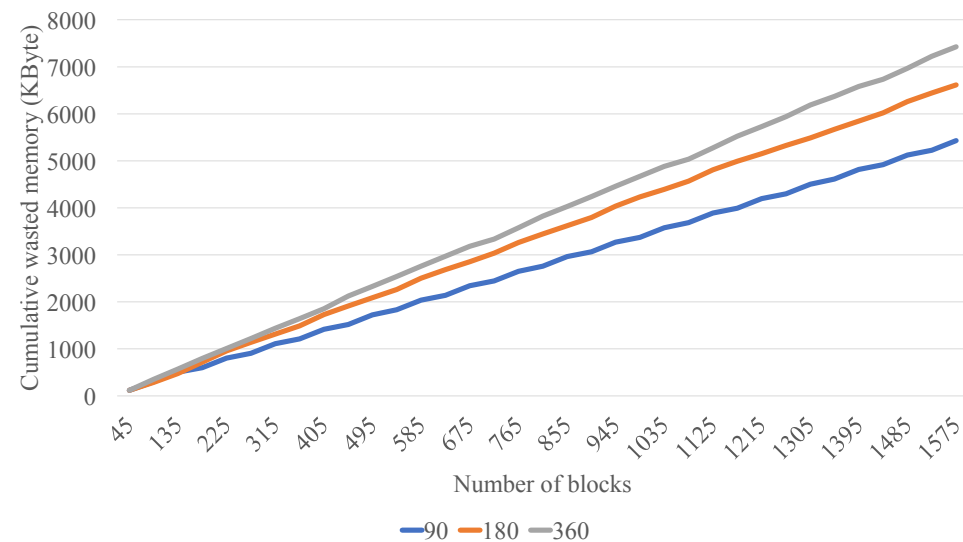
An analysis on attack likelihood and attack resistance of MOF-BC based on ETSI.

Attack	Resistance to attack	Attack likelihood
Transaction removal	Beyond high	Unlikely
False Storage Claim	Moderate	Possible
Eclipse attack	Moderate	Possible
Malicious SP	Basic	Likely
Colluding attack	Beyond high	Unlikely
Reward tracking	Beyond high	Unlikely
Malicious Agents	High	Unlikely

Performance Evaluation



Evaluating the impact of CP on BC size

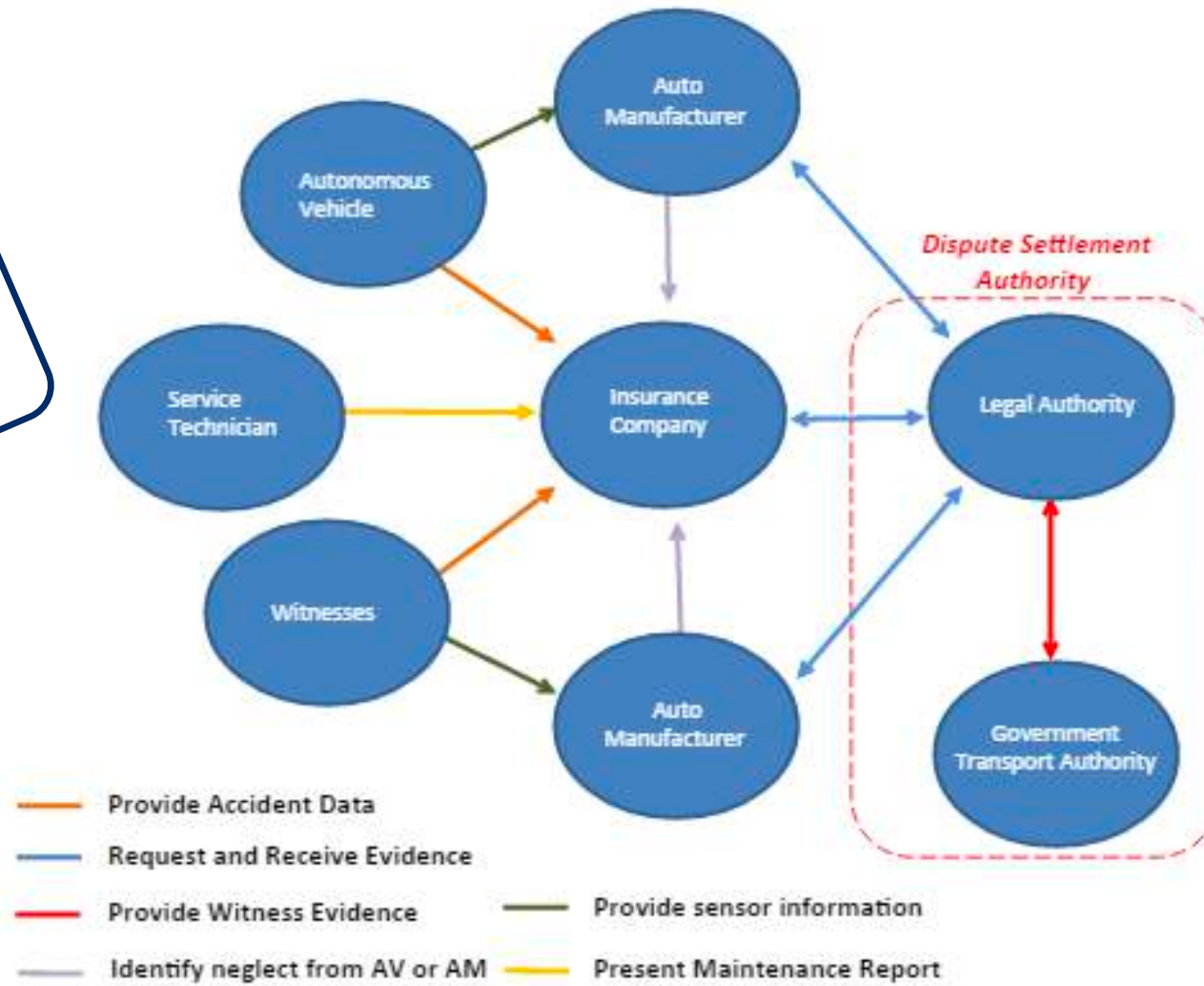


Evaluating cumulative wasted memory

Liability Attribution Framework



A Permitted Approach



Trust?



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

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

"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."

Improving Trust

Conventionally



Social institutions or relations



Trusted third parties

With Blockchain



Trust in the code

Trust machines

Application Assets and Domains

	Assets		Domain	
	digital	tangible	finance	other
Governmental services				
– Registry of deeds, eVoting, ...	X	X	(X)	X
Trading/banking services				
– Diamonds, cash-heavy, ...	X	X	X	(X)
Copyright				
– Authorship, ownership, ...	X	(X)		X
Data and identity management				
– Records, processes, compliance	X	(X)		X
“Chain” support/IoT services				
– Supply, food, energy, ...	(X)	X	X	X
eEntertainment	X			X
Cryptocurrencies	X		X	

Improving Trust

A blockchain record may represent **the true state of reality** – true for virtual assets

- e.g. Bitcoin generation, Ether transfer
- created on the chain, can be proven using the protocol


The blockchain ensures that the record is immutable AND trusted

Improving Trust

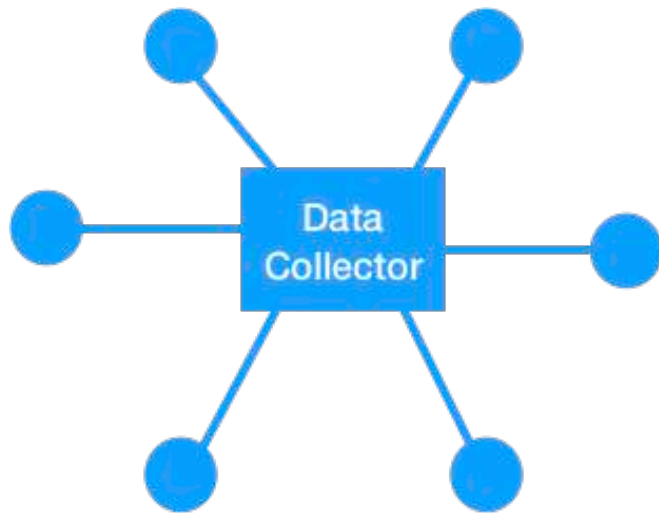
In IoT, a blockchain record represents an **observation of reality** – true for physical assets

- e.g. recording a sensor measurement on blockchain
- created off-chain, cannot be proven by simply examining the blockchain

The blockchain ensures that the record is immutable

- No guarantees for the correctness of the measurement
- Provides trust in a record of  data

untrusted



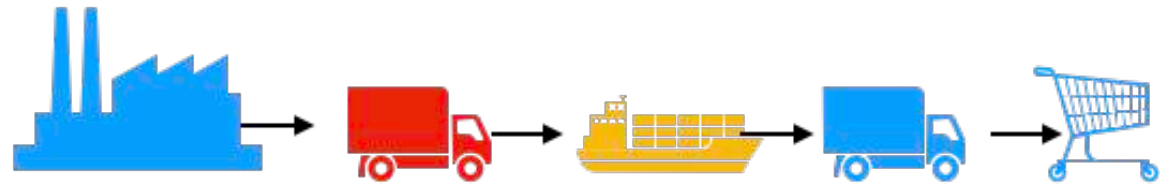
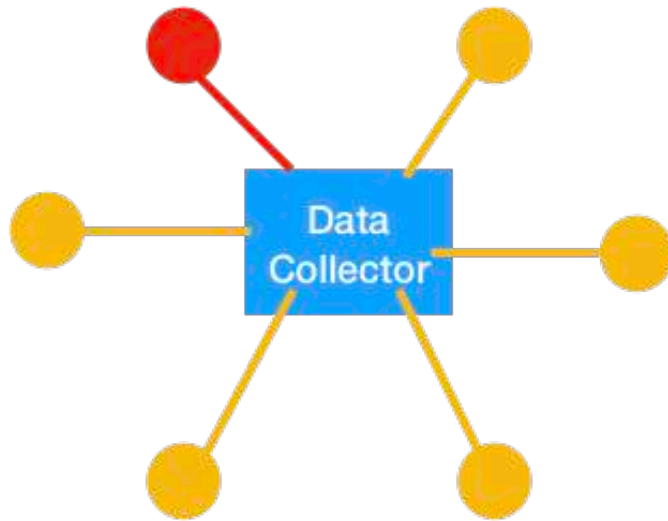
Trust in the IoT data improved by

- comparing it with the neighbour nodes
- comparing with the record history



Trust in the supply chain

- verification at points of transfer



K. Guan, S. Dehnie, L. Gharai, R. Ghanadan and S. Kumar, "Trust management for distributed decision fusion in sensor networks," *2009 12th International Conference on Information Fusion*, Seattle, WA, 2009, pp. 1933-1941.

Jiang, Jinfang, et al. "An efficient distributed trust model for wireless sensor networks." *IEEE Transactions on Parallel & Distributed Systems* 1 (2015)