Blockchain for Cyberphysical Systems

Salil Kanhere

School of Computer Science and Engineering

UNSW Sydney, Australia

E: salil.kanhere@unsw.edu.au

in: www.linkedin.com/in/salilkanhere

Sidra Malik
UNSW & CSIRO

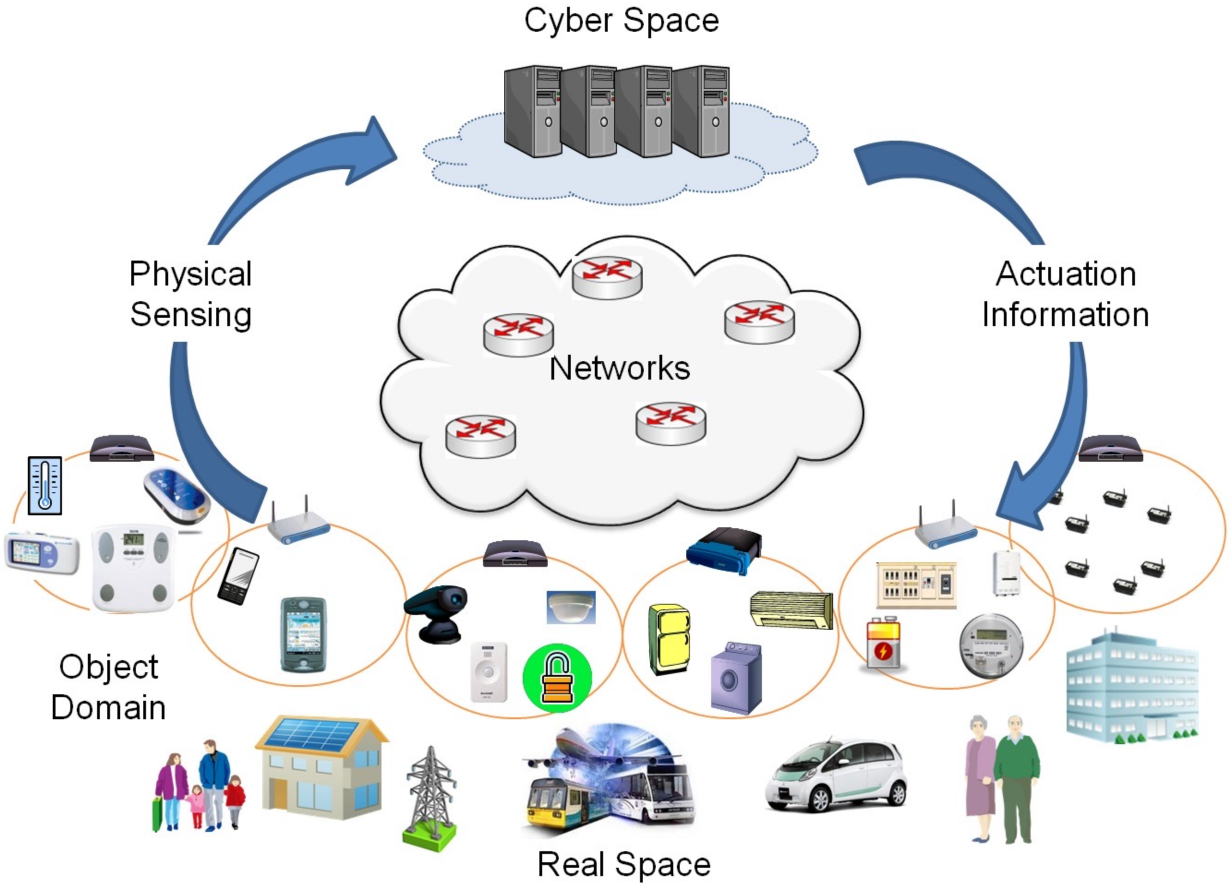
Volkan Dedeoglu
CISRO

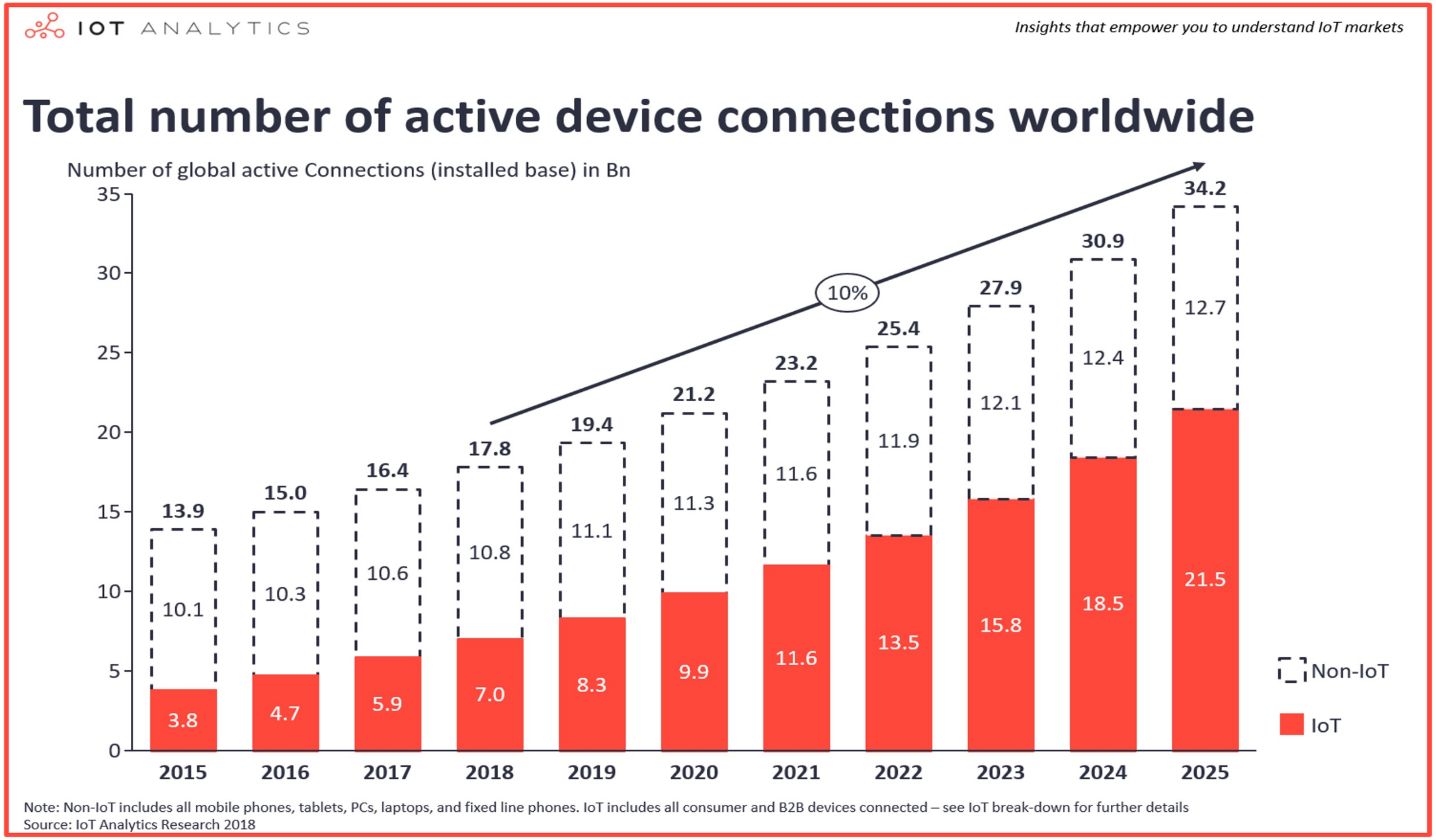
Raja Jurdak
QUT

Guntur Dharma Putra, UNSW

UNSW SYDNEY

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

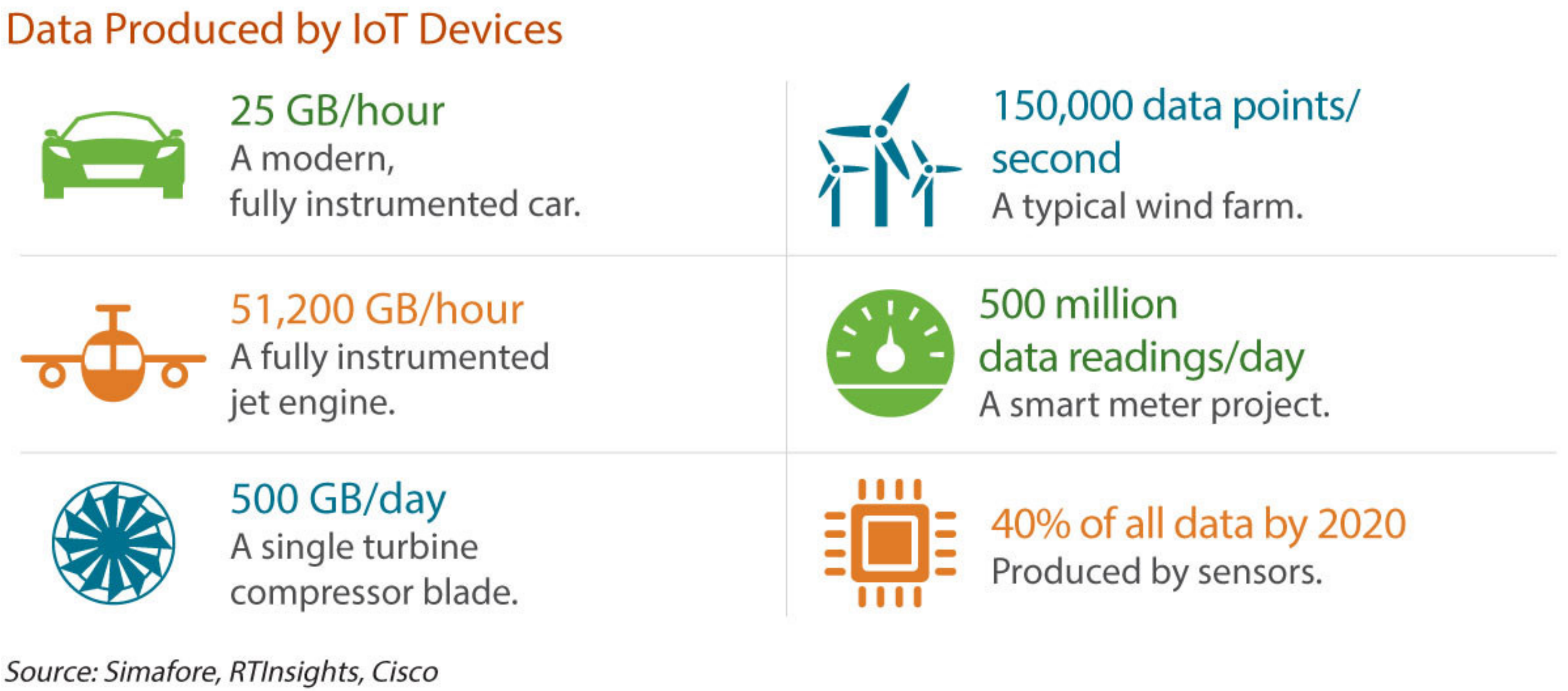




IOT ANALYTICS
Insights that empower you to understand IoT markets
Total number of active device connections worldwide
Number of global active Connections (installed base) in Bn
35
30
25
20
15
10
5
0
10%
13.9
15.0
16.4
17.8
19.4
21.2
23.2
25.4
27.9
30.9
34.2
10.1
10.3
10.6
10.8
11.1
11.3
11.6
11.9
12.1
12.4
12.7
3.8
4.7
5.9
7.0
8.3
9.9
11.6
13.5
15.8
18.5
21.5
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
Non-IoT
IoT
Note: Non-IoT includes all mobile phones, tablets, PCs, laptops, and fixed line phones. IoT includes all consumer and B2B devices connected – see IoT break-down for further details
Source: IoT Analytics Research 2018

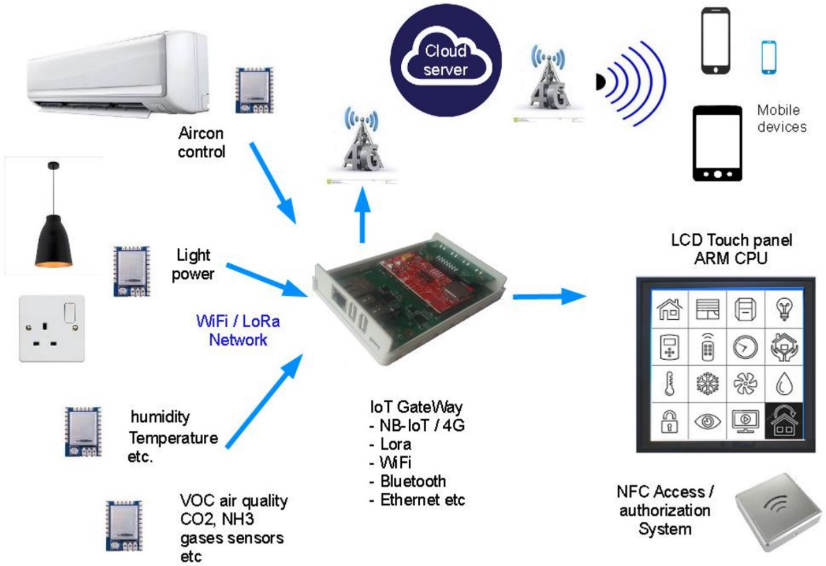
UNSW SYDNEY

Data Tsunami

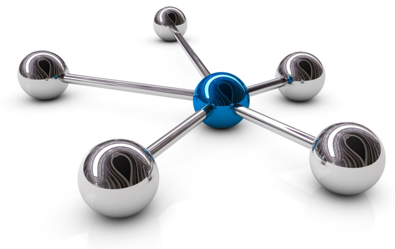


Current IoT/CPS Ecosystems

- 3 Tiers:
- Low-power IoT devices
- Gateway
- Cloud



Centralization does not scale

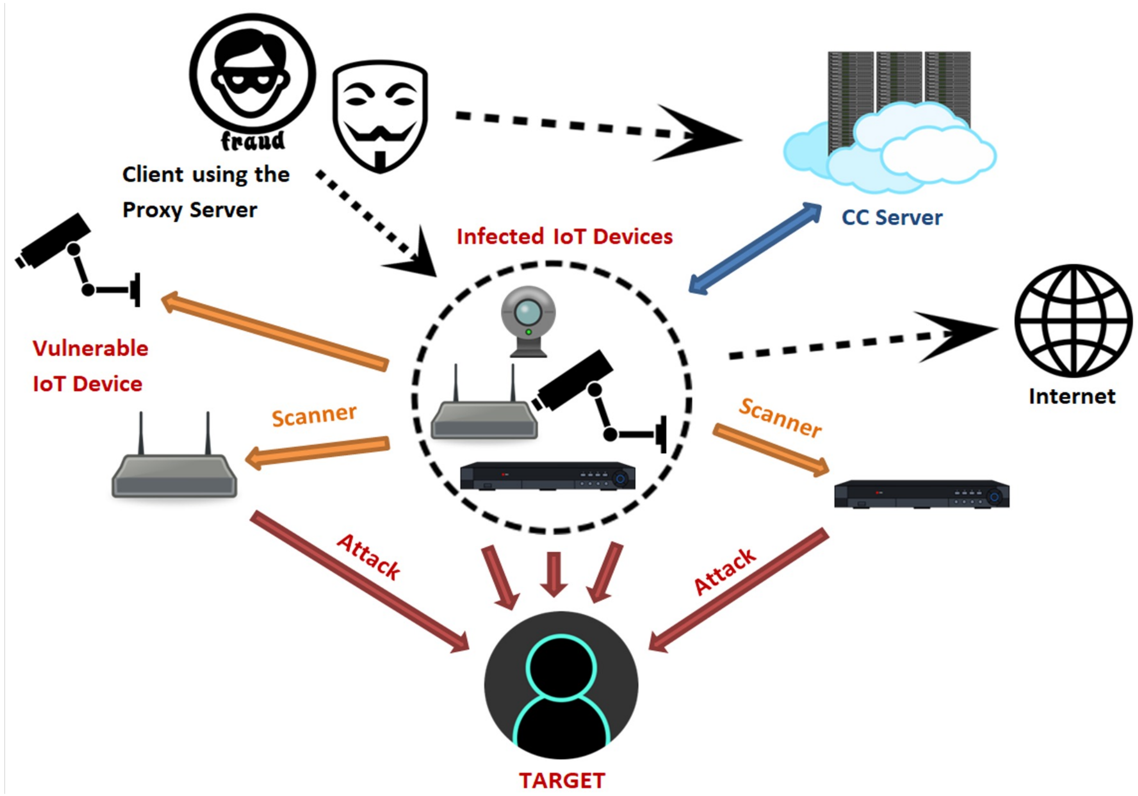


Centralised brokered communication models based on the client-server paradigm

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 is a significant challenge



Mirai Botnet

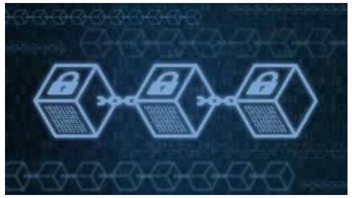
Establishing trust can be difficult

- CPS ecosystems are very complex
- Many actors with different objectives and possibly conflicting goals

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
- Difficult to establish trust across complex CPS ecosystems
- Complex interactions of different OS/software stacks/hardware
- Poor implementation of security/privacy mechanisms
- ……..

Salient Features of Blockchain



- Tamper-proof storage of information
- Auditability/Transparency
- No reliance on third-parties
- Distributed Trust
- Data provenance
- Cryptographically secure
- Smart contracts can automate numerous processes

Blockchain for Cyberphysical Systems

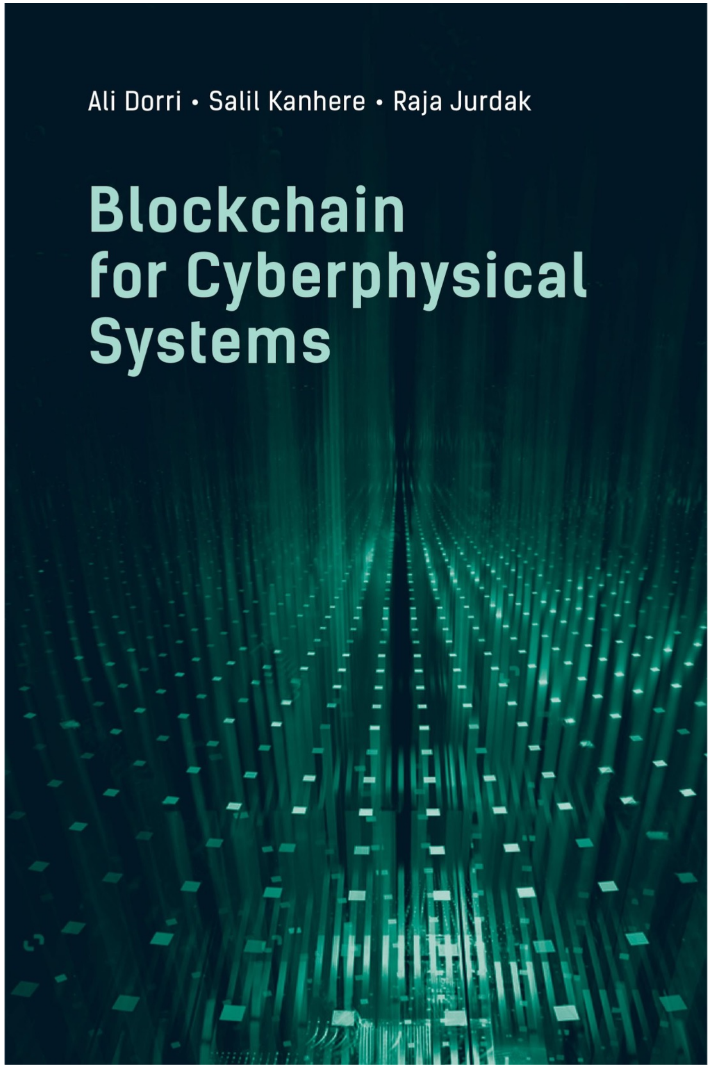
Ali Dorri, Salil Kanhere, Raja Jurdak

Copyright: 2020

Pages: 290

ISBN: 9781630817831

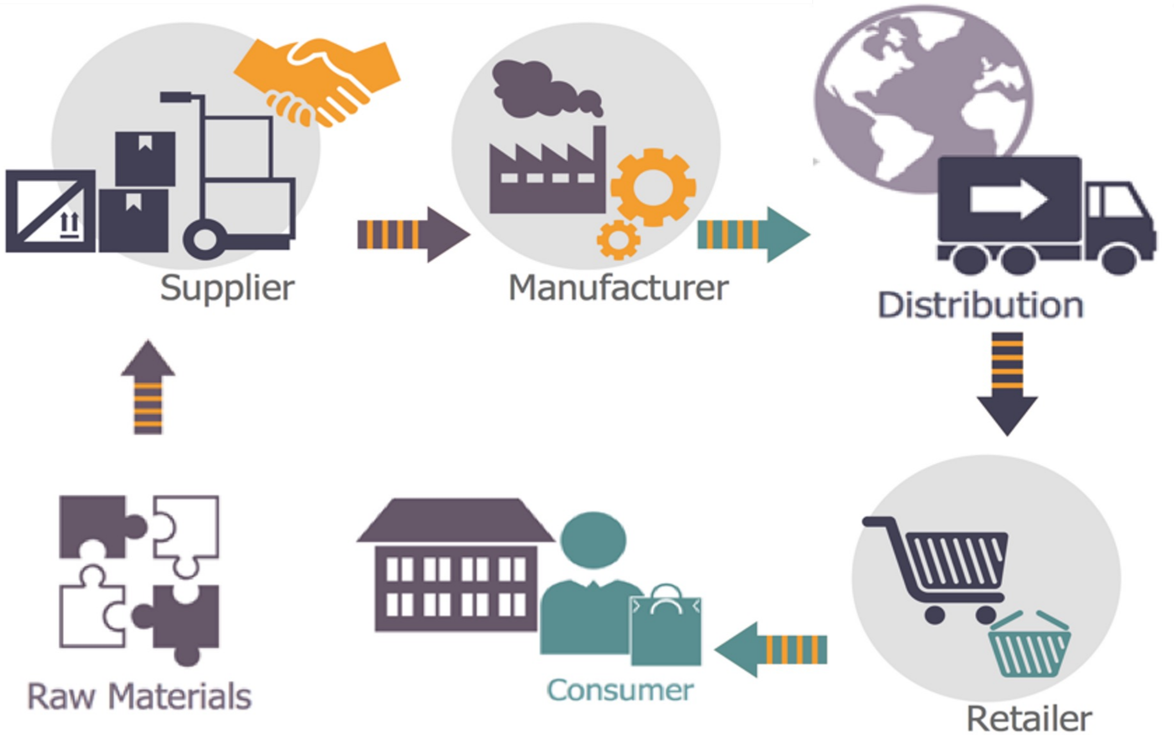
Artech House, USA/UK



Supply Chain Lifecycle

A system of organizations, people activities, involved in the distribution of raw material or finished goods

- Food
- Pharmaceutical
- Aerospace and Defense
- Practically any consumer goods



Traceability

Counterfeiting

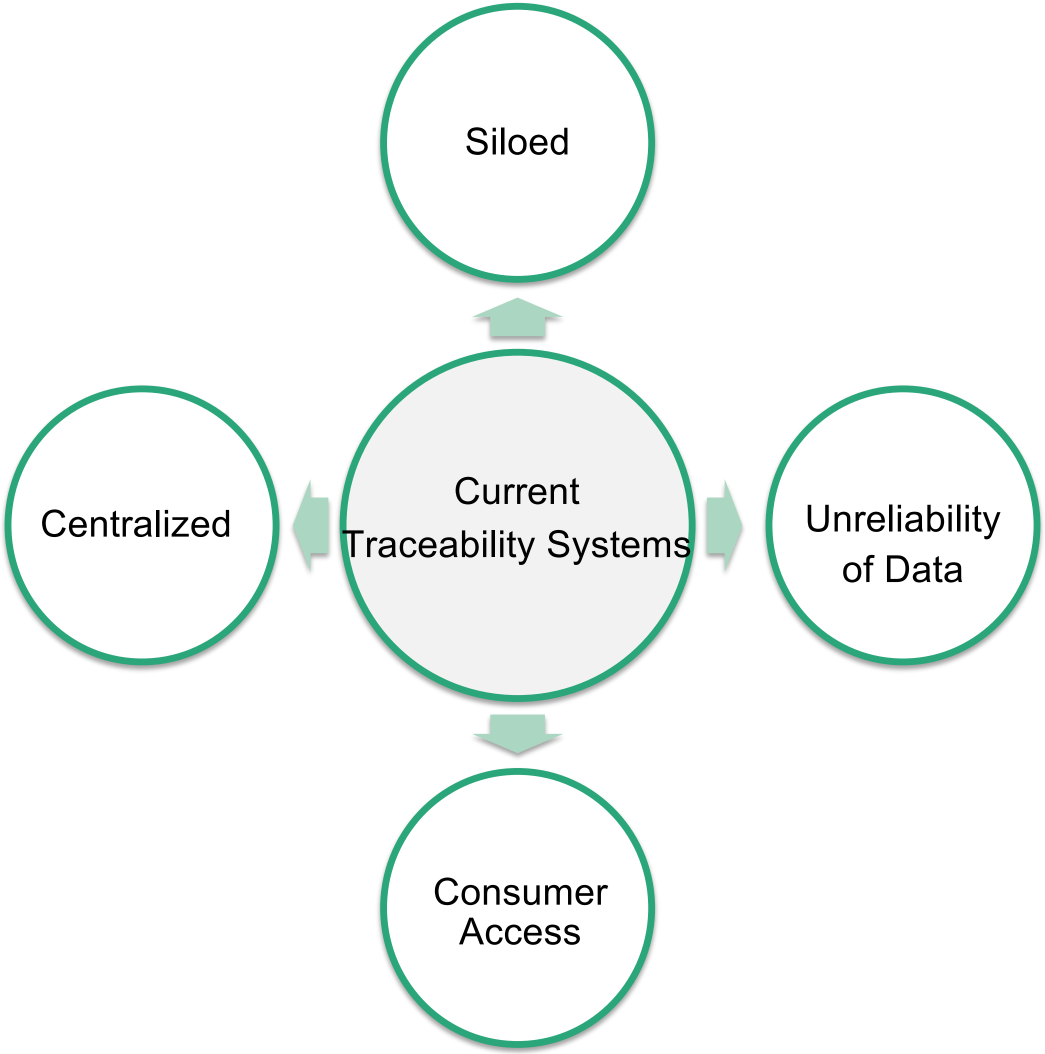
Needles in Strawberries

Two dead from listeria linked to smoked salmon

Two elderly people have died. Source: Getty

Contaminated smoked salmon from Tasmania is the likely cause of two fatal listeriosis cases in New South Wales and Victoria.

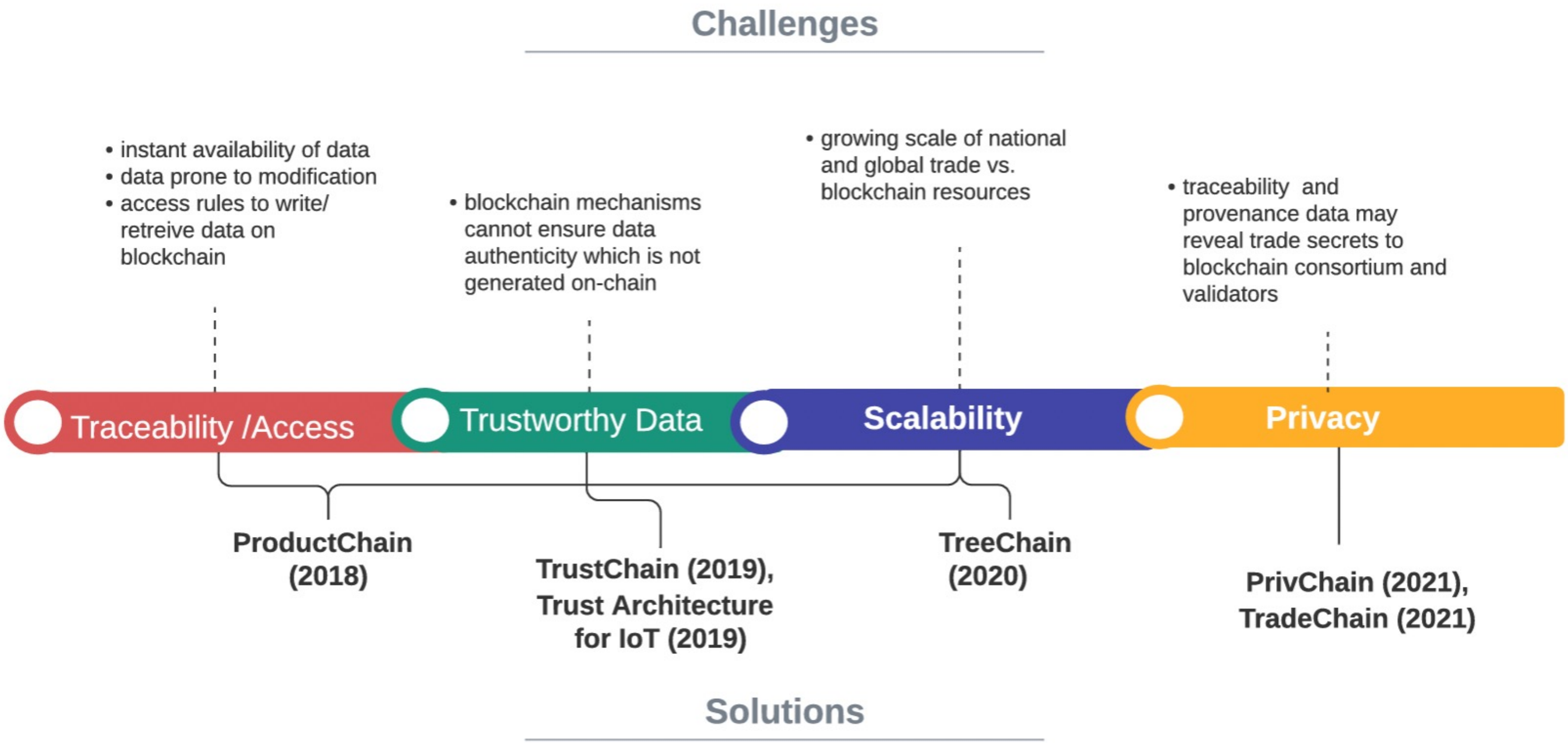
Farm to Fork


Siloed
Centralized
Current Traceability Systems
Unreliability of Data
Consumer Access


ISSUES

UNSW SYDNEY

Challenges and Solutions



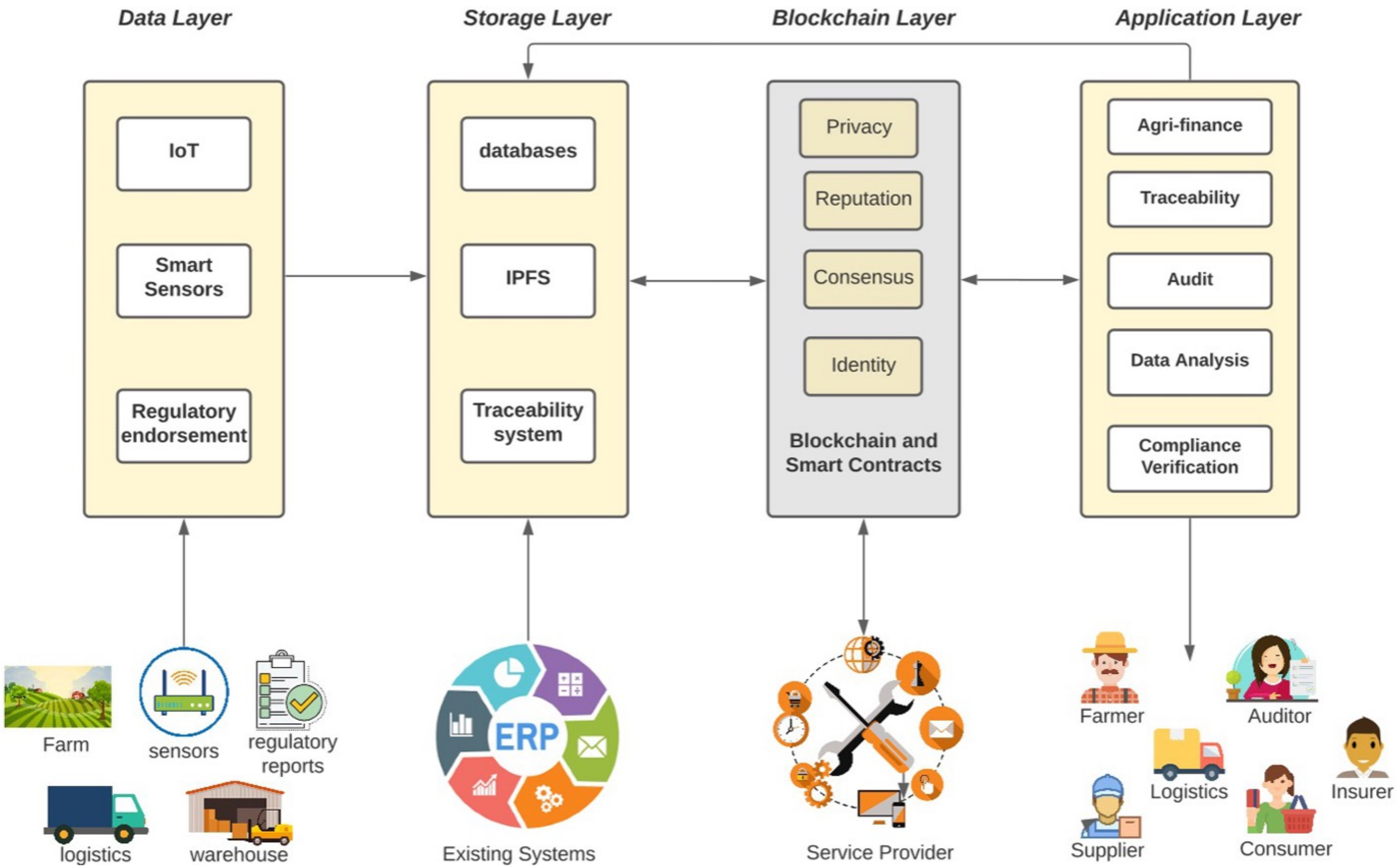
ProductChain - Overview

- Holistic approach, **Consortium** to manage a **permissioned blockchain**
- **Transaction Vocabulary**
  - Integration of IoT data from embedded sensors
  - 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 17th IEEE Symposium on Network Computing and Applications (NCA), Boston, November 2018.

UNSW SYDNEY

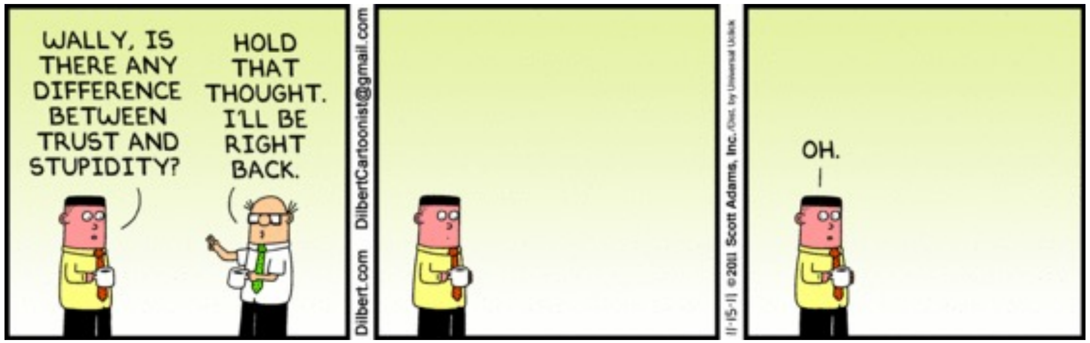
ProductChain Architecture



Trust: Challenges

- How do we trust data written into the blockchain?
  - Hashed data on the blockchain represents digital observations of physical events

- Need for a trust management system with the following requirements
  - Multi-faceted assessment of trustworthiness of logged data
  - Flexibility for ascribing trust to the supply chain entities and commodities and at different granularities



TrustChain: Contributions

BC-based **reputation/trust framework**

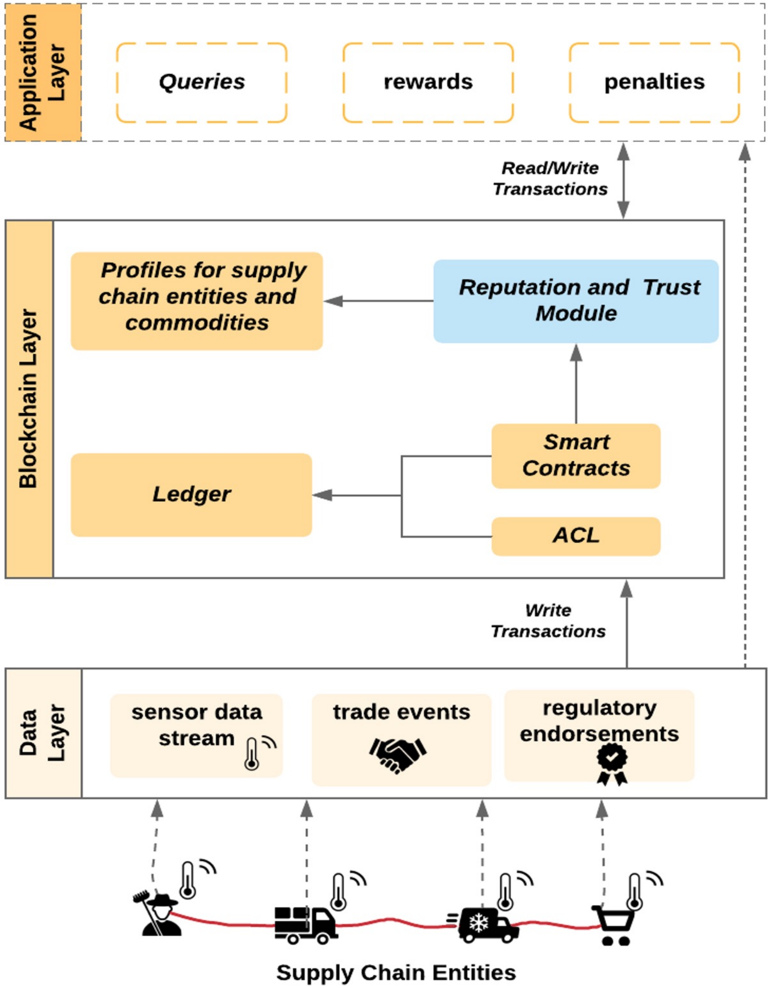
Flexible and granular

Smart contracts for **automation**

Accountability mechanisms

Hyperledger Fabric **Implementation**

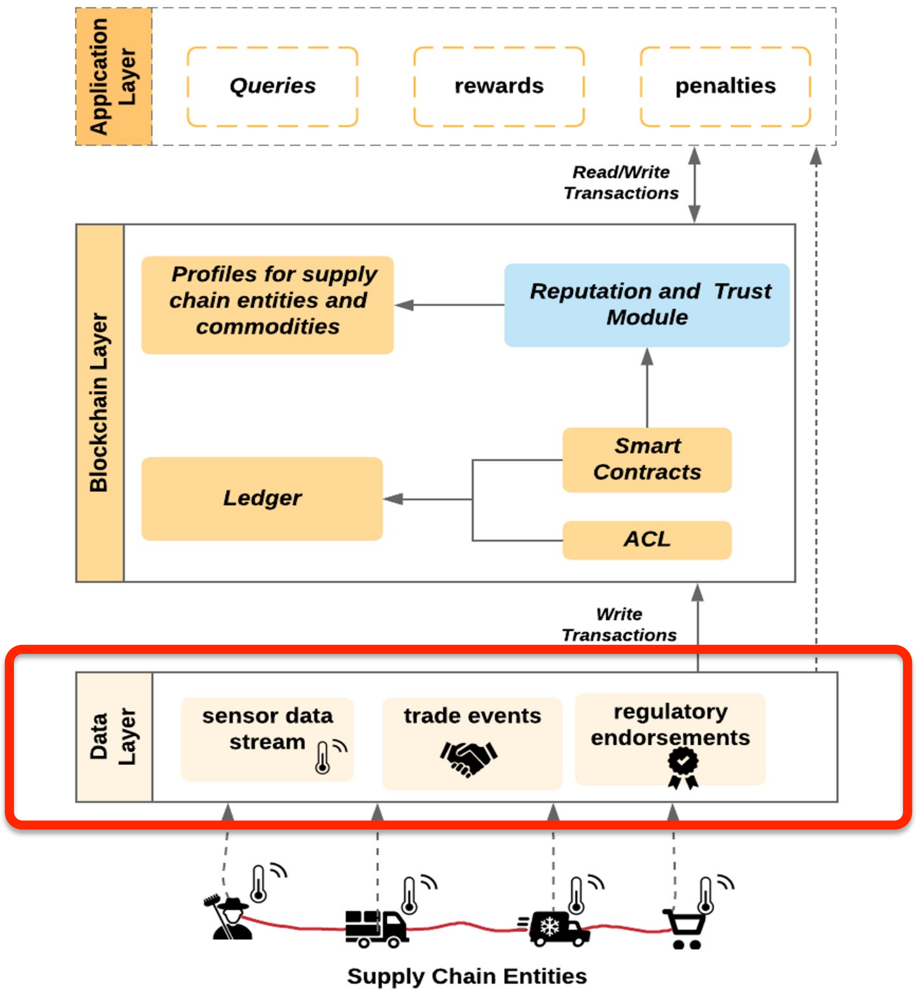
Minimal **overheads**



S. Malik, V. Dedeoglu, S. S. Kanhere and R. Jurdak, TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains, in Proceedings of the IEEE International Conference on Blockchain, Atlanta, July 2019

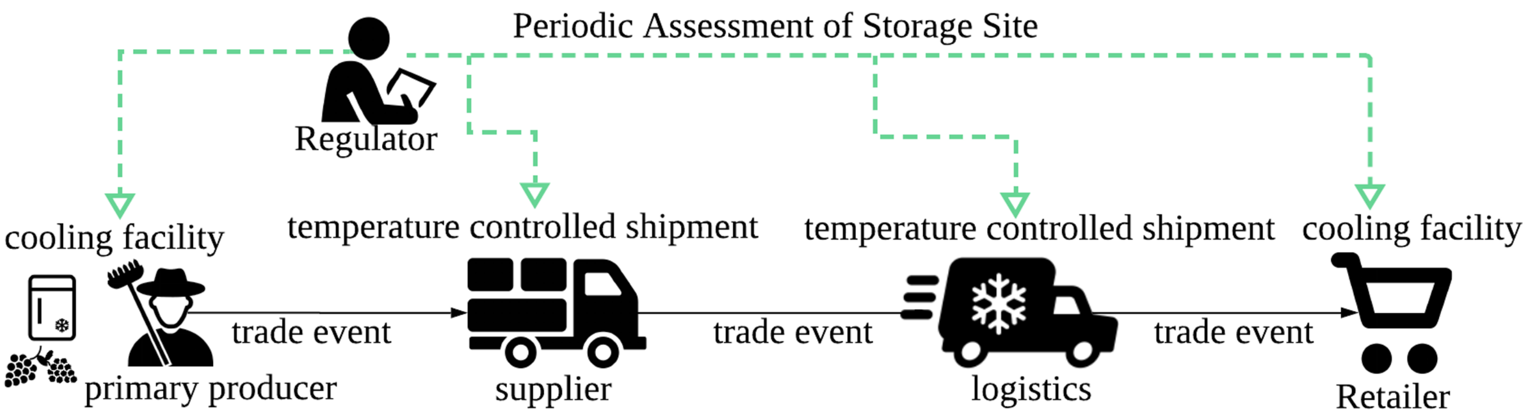
TrustChain

Data Layer



TrustChain

Data Layer

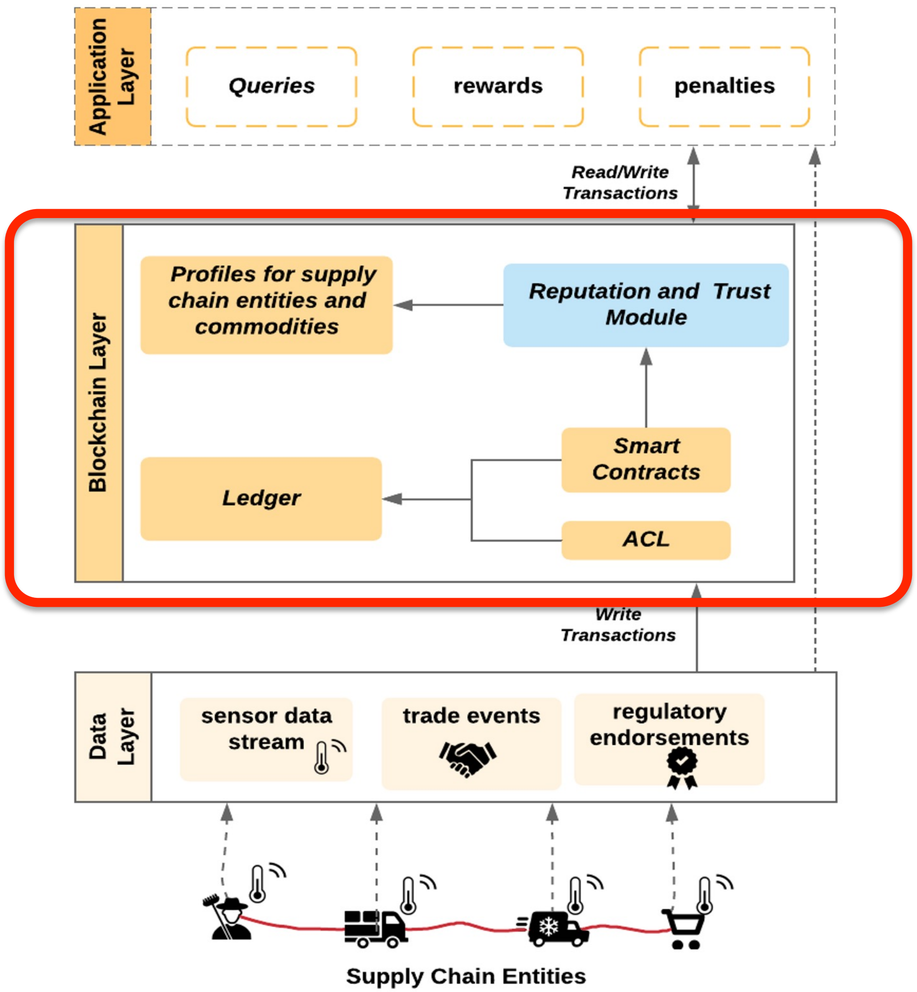


Multi-sourced Data Observations:

- Sensors
- Buyer's Rating (in a trade event)
- Regulatory Bodies

TrustChain

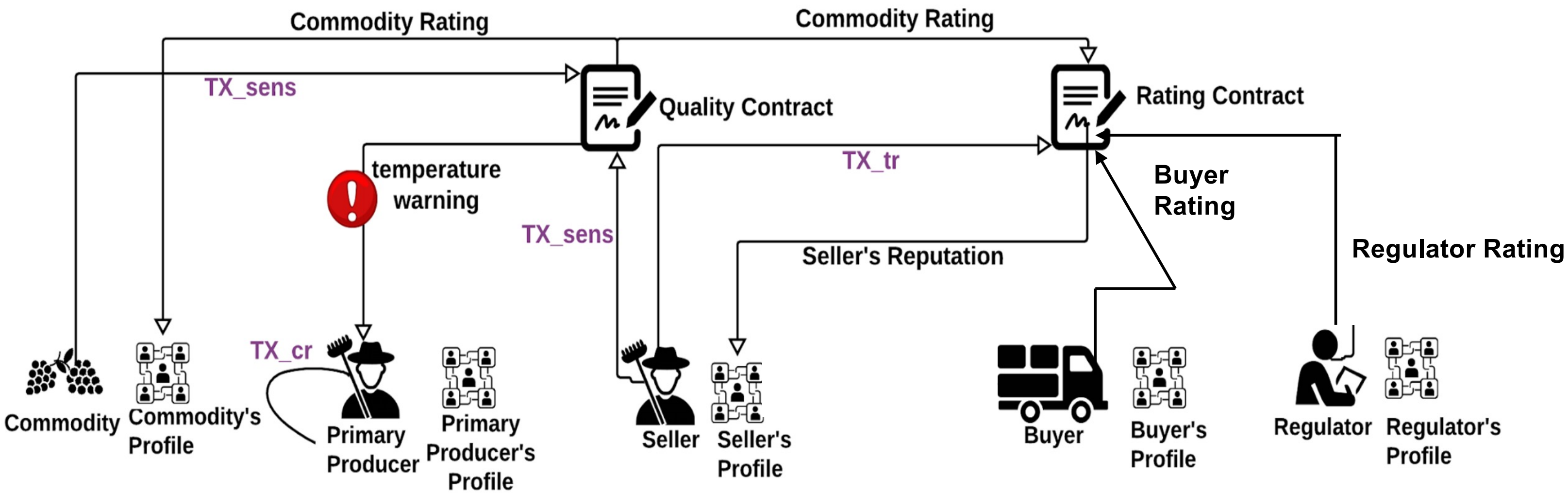
Blockchain Layer



TrustChain

Blockchain Layer

Smart Contracts



Reputation and Trust Model

DeTRM: Trust and Reputation Model

Commodity trust is based on sensor data

$$\mathbf{V}^n = \begin{bmatrix} v_{11}^n & v_{12}^n & \dots & v_{1p}^n \\ v_{21}^n & v_{22}^n & \dots & v_{2p}^n \\ \vdots & \vdots & \ddots & \vdots \\ v_{o1}^n & v_{o2}^n & \dots & v_{op}^n \end{bmatrix}$$

and $\widehat{t}_{n,q}$ is calculated as follows:

$$\widehat{t}_{n,q}(o,p) = \frac{(1-\gamma)}{p} \sum_{i=1}^{o} \sum_{j=1}^{p} \gamma^{(o-i)} \delta_{j,i} \mathcal{V}_{j,i}^{C} \mathcal{V}_{j,i}^{E}$$

where

$$\delta_{j,i} = \begin{cases} \delta_{max}, & \text{if } \mathrm{T}_{min} < \mathcal{V}_{j,i} < \mathrm{T}_{max} \ , \\ \delta_{min}, & \text{otherwise,} \end{cases}$$

Participant trust is based on buyer feedback

$$\widehat{T}_n(r) = (1-\gamma) \sum_{i=1}^{r} \gamma^{(r-i)} \sigma_i$$

$$\sigma_i = \frac{1}{|\mathbf{tc}_i|} \sum_{tc_j \in \mathbf{tc}_i} \psi_{tc_j} tc_j$$

Participant reputation is weighted average of commodity trust, participant trust and regulator rating

$$\widehat{R}_n(q,r,u) = \frac{w_t}{|\widehat{\mathbf{t}}_n|} \sum_{\widehat{t}_{n,q} \in \widehat{\mathbf{t}}_n} \widehat{t}_{n,q} + w_T \widehat{T}_n(r) + w_e \widehat{E}_n(u)$$

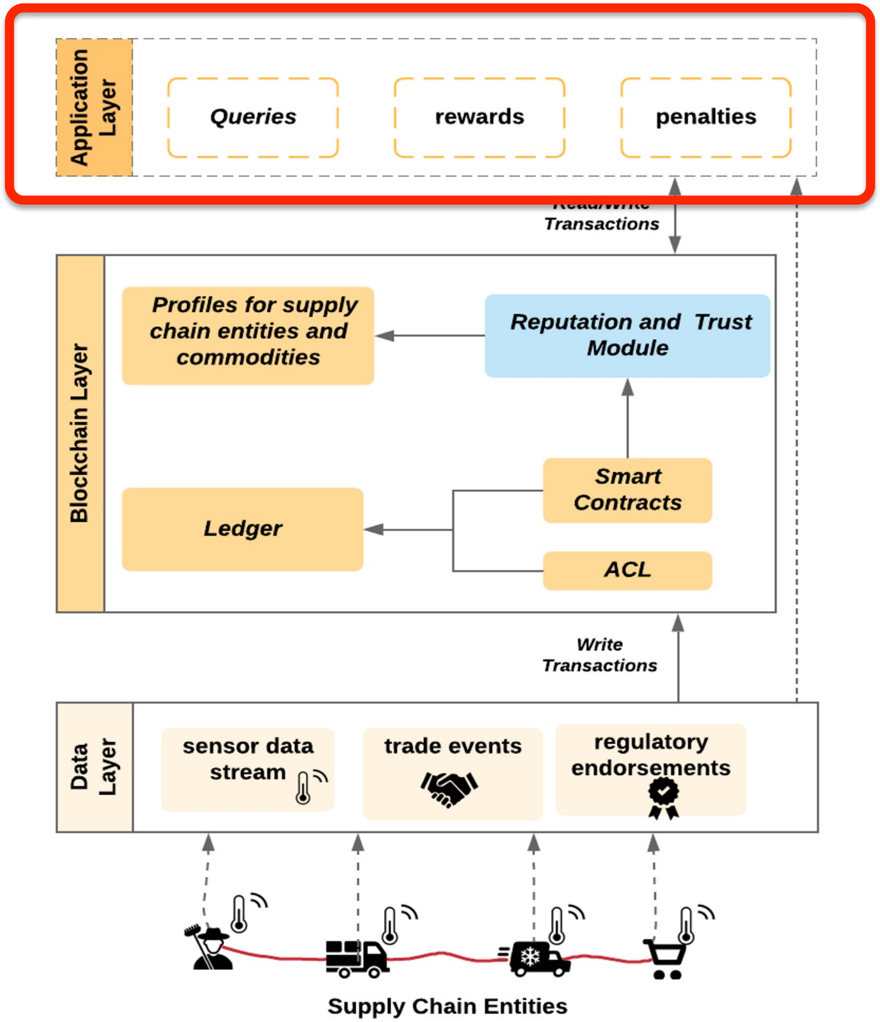
where

$$\widehat{E}_n(u) = (1-\gamma) \sum_{i=1}^{u} \gamma^{(u-i)} e_i$$

G. D. Putra,C. Kang, S. S. Kanhere and J. W. K. Hong, DeTRM: Decentralised Trust and Reputation Management for Blockchain-based Supply Chains, in Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), virtual, May 2022

TrustChain

Application Layer



TrustChain

Application Layer

Queries

- Computing trust rating for supply chain entities and reputation of commodity
- Properties of commodities and traders

Rewards

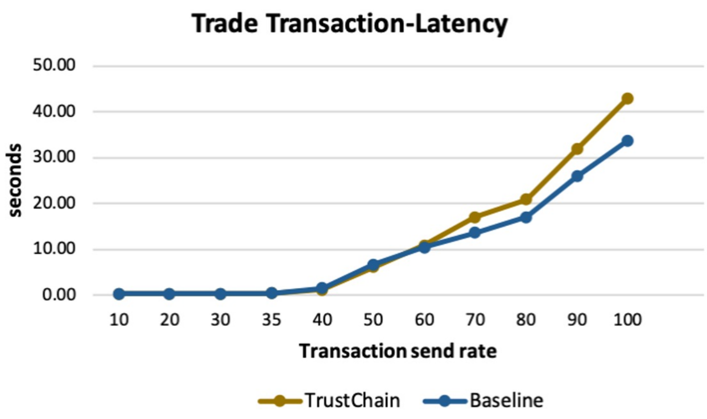
- Incentivizing honest traders

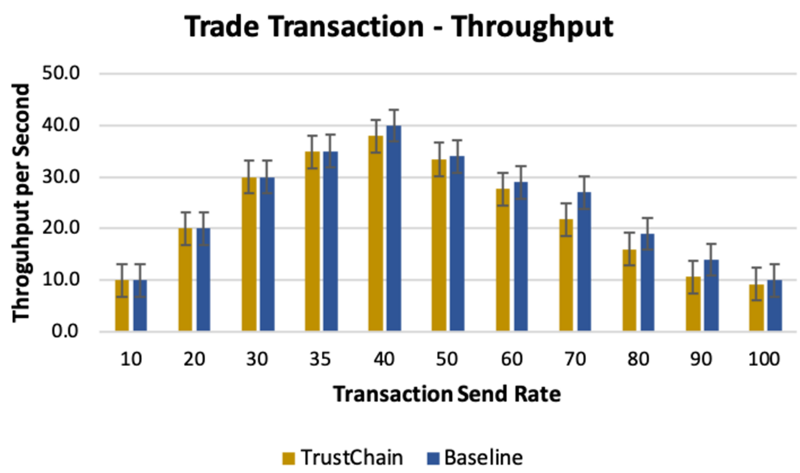
Penalties

- Penalize dishonest behaviour

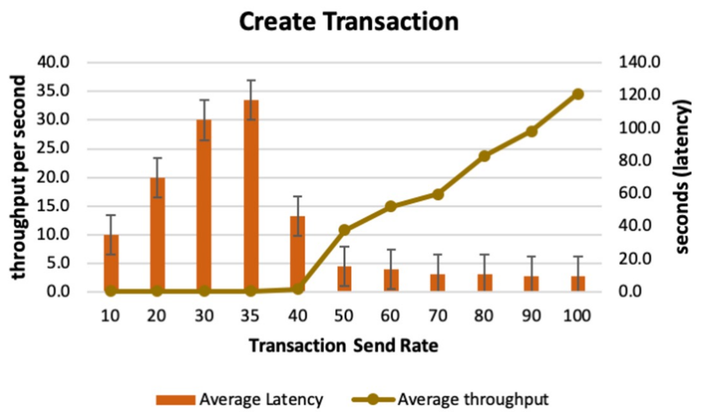
TrustChain: Evaluations

Throughput and Latency vs. Transaction Send Rate

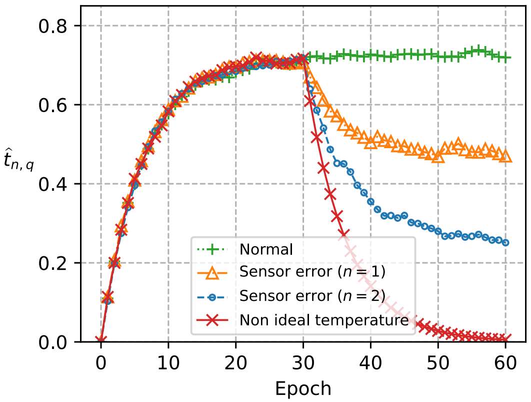


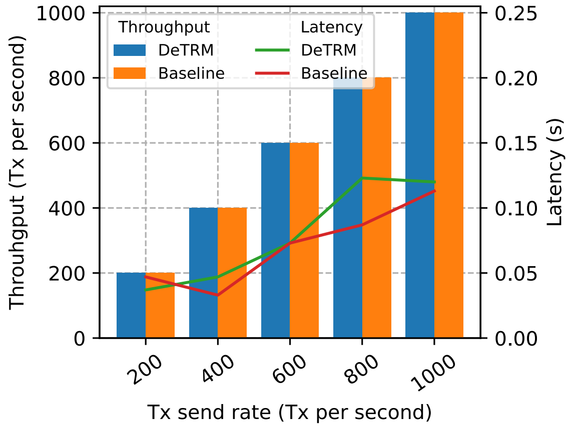


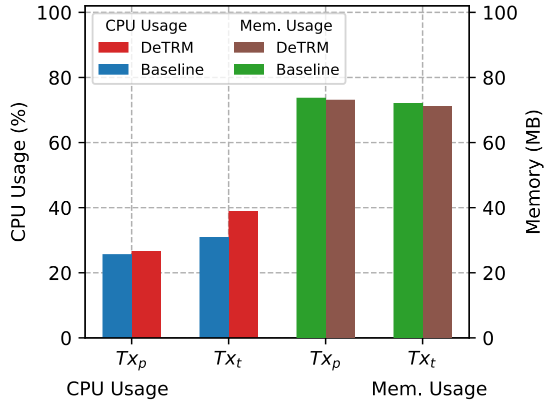
Throughput and Latency vs. Transaction Send Rate



DeTRM: Evaluations







Trust evolution ($t_{n,q}$) of assets stored in various conditions.

The trust decline is unique for each non-ideal condition.

The throughput and latency against the baseline (plain SCMS w/o TRM).

Our solution incurs negligible overheads with similar throughput.

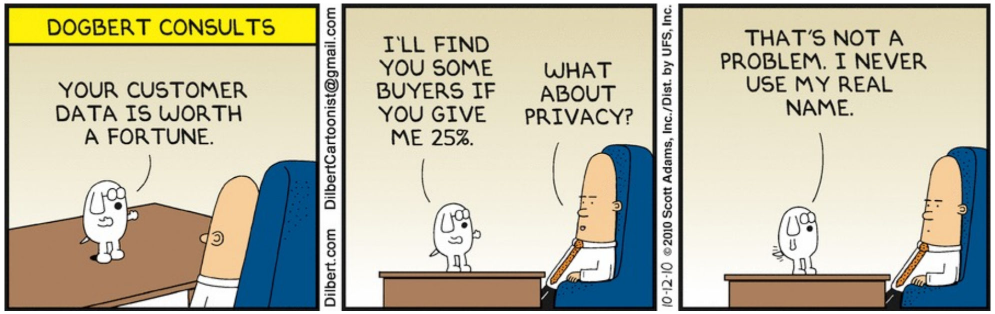
The CPU and memory usage against the baseline (plain SCMS w/o TRM).

Minimal and insignificant overheads are observed.

Privacy: Challenges

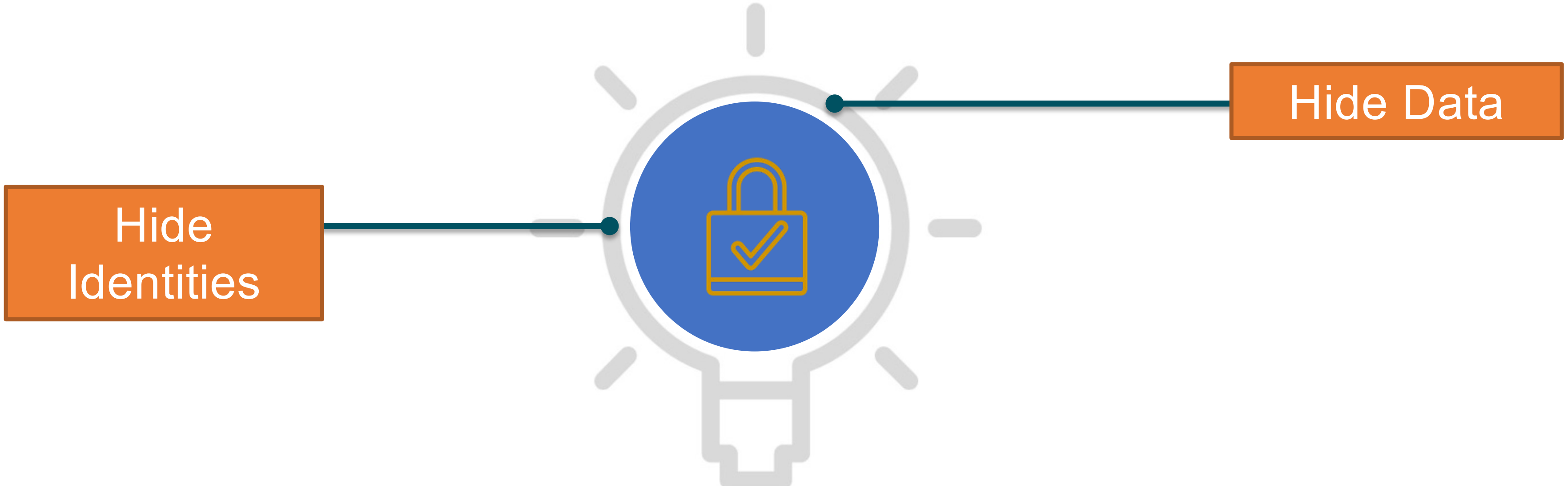
Traceability

Privacy



Privacy Preservation

Issues



Privacy Preservation

Solution

Hide Identities

Use multiple identities for trade

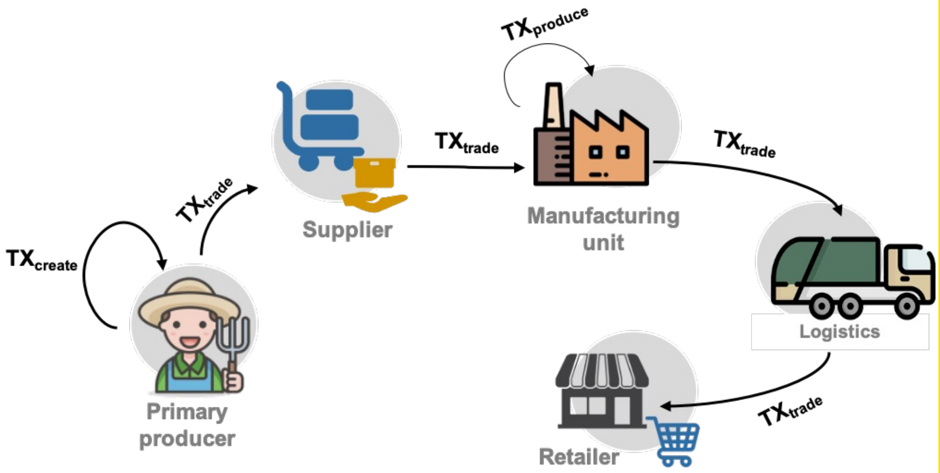
TradeChain

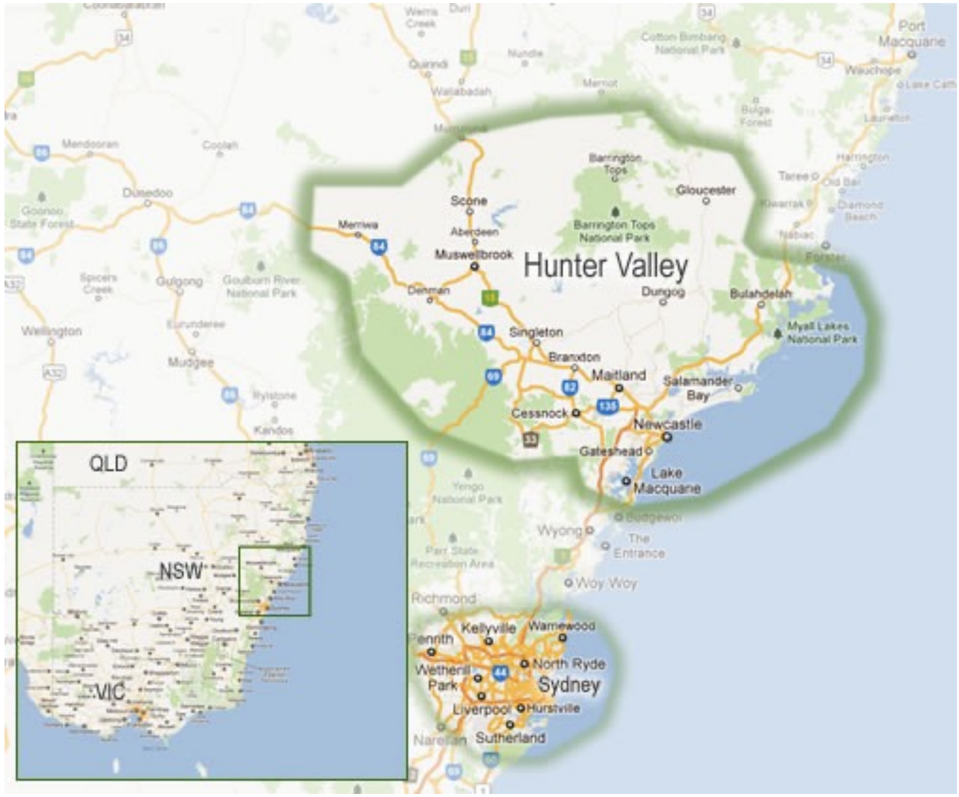
Hide Data

Share Proofs on Data

PrivChain

PrivChain: Use-case





S. Malik, V. Dedeoglu, S. S. Kanhere and R. Jurdak, PrivChain: Provenance and Privacy Preservation in Blockchain enabled Supply Chains, in Proceedings of the IEEE International Conference on Blockchain, Helsinki, August 2022

UNSW SYDNEY

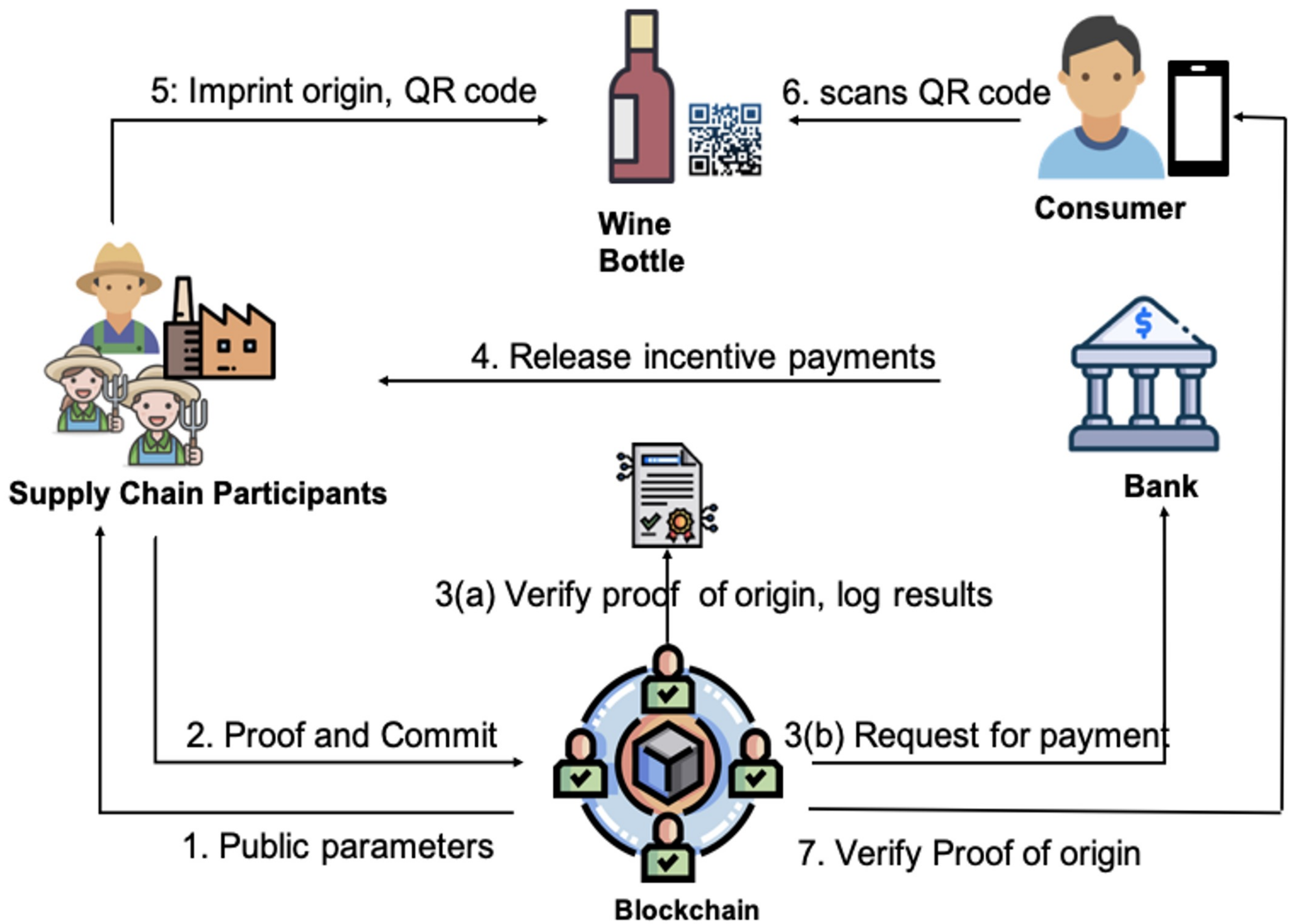
PrivChain: Key Contributions

- **Zero-Knowledge Proof (ZKP) based privacy preservation** solution where proof of provenance is provided without disclosing privacy-sensitive data

- **Automated verification** of the provenance proofs and the integration of the **incentive mechanism** that enforces instant rewards

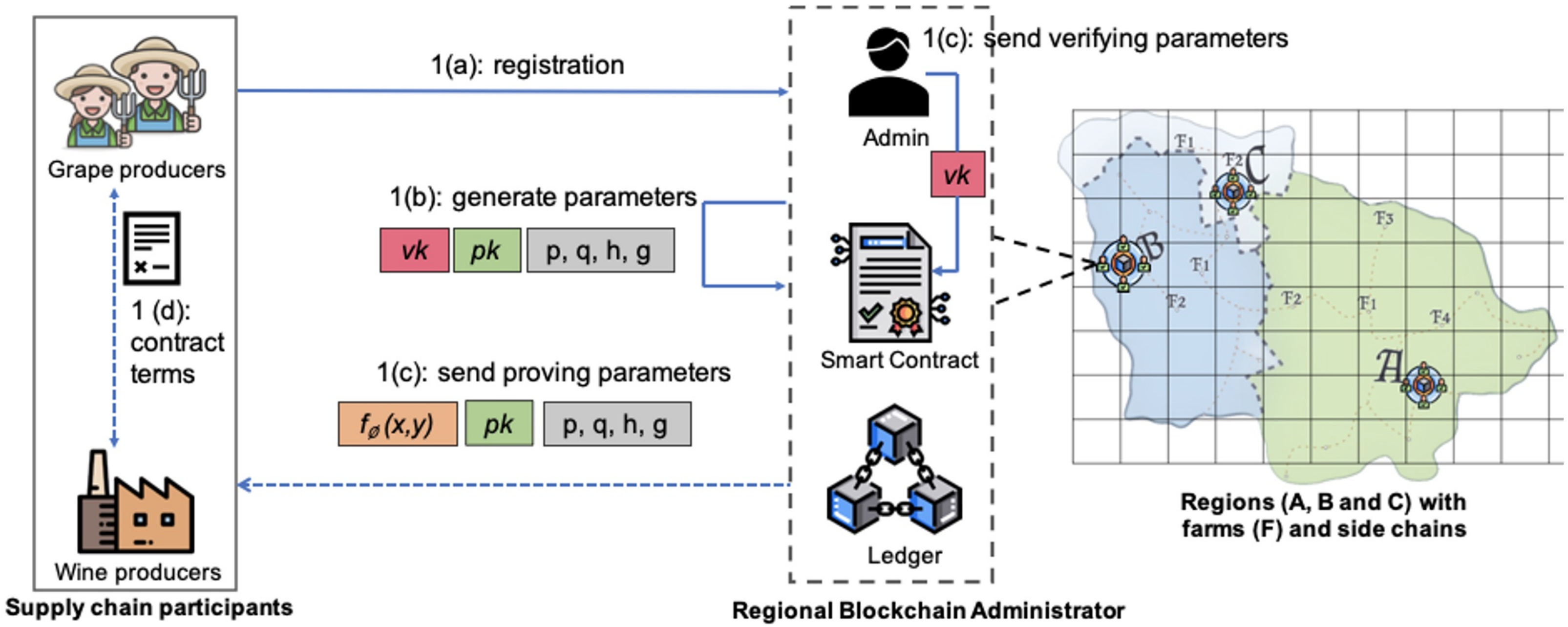
- Proof of concept implementation with **minimal overheads** for proof verification

PrivChain
Framework



PrivChain

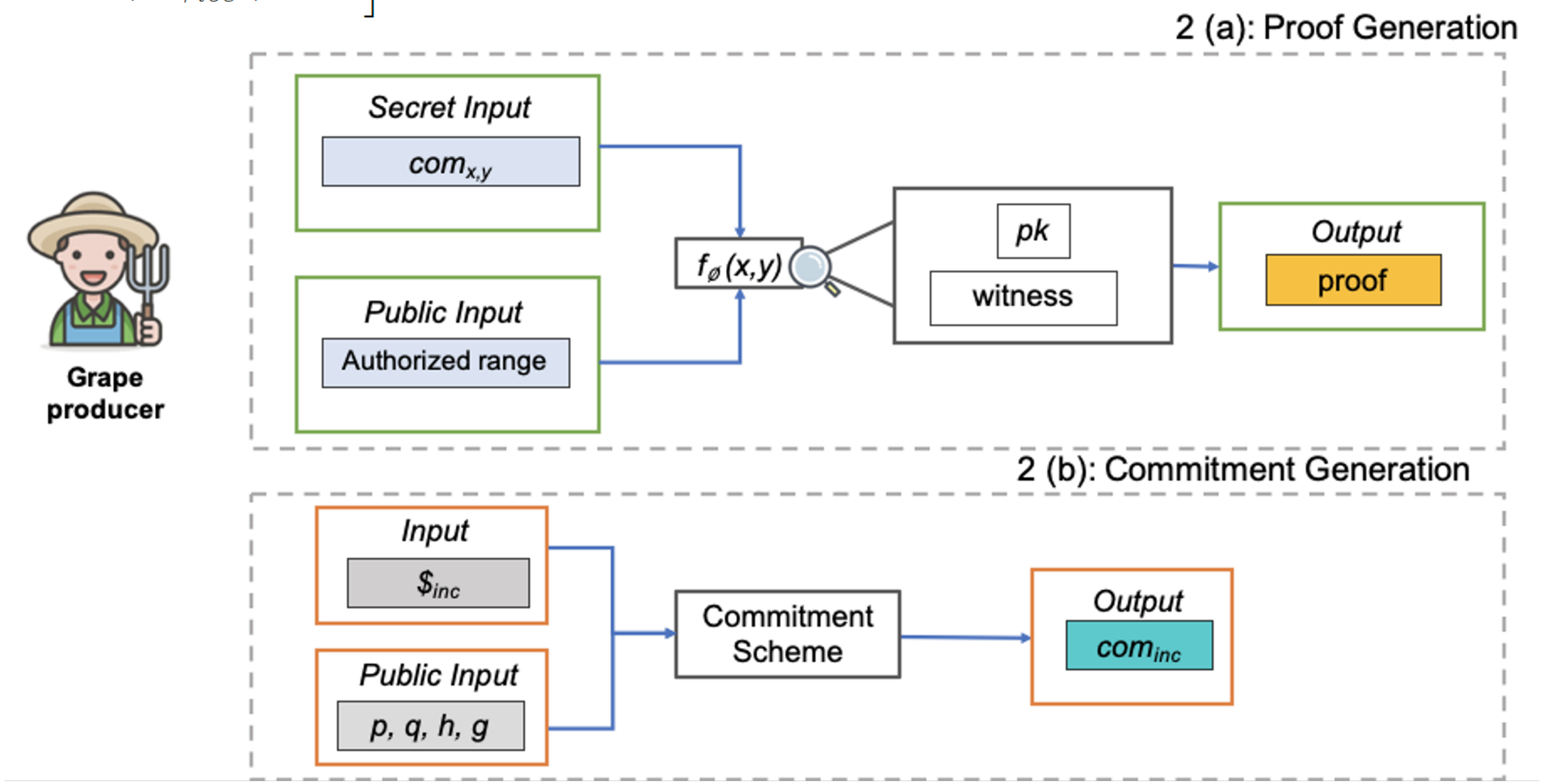
Setup



PrivChain

Proof Generation

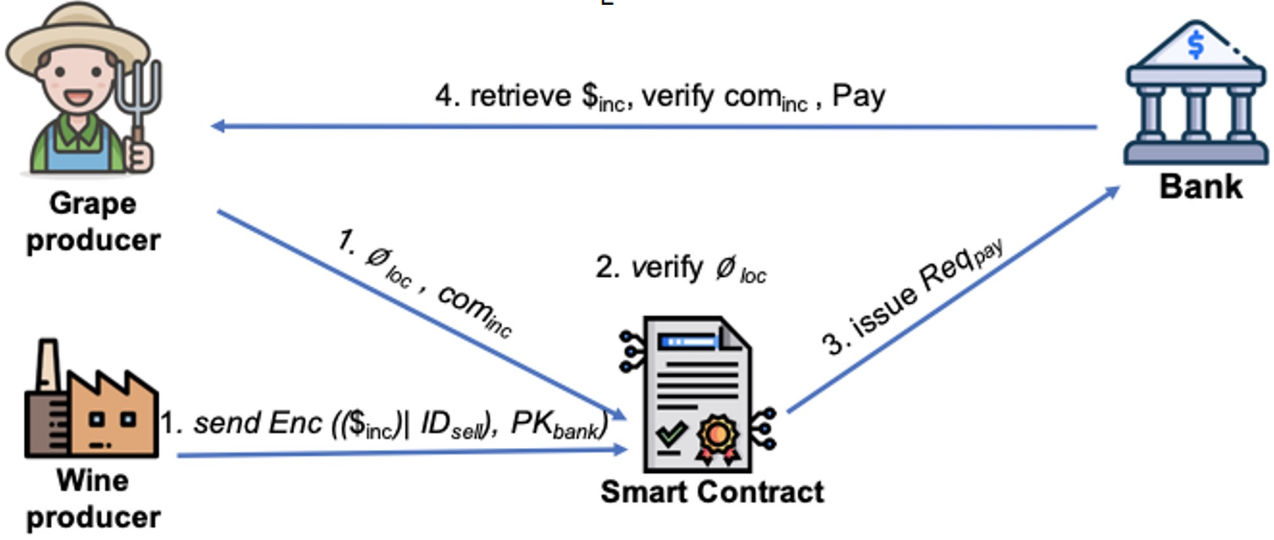
$$TX_{cr} = \left[\ ID_g \mid H_{data} \mid L_{\phi_{loc}} \mid Sig_s\ \right]$$



PrivChain

Proof verification and Incentive Payments

$$Req_{pay} = \left[com_{inc} | Enc((\$_{inc} | r | ID_{sell}), PK_{bank}) | Sig_{buy}\right]$$



$$TX_{trade} = \left[ID_g \,|\, H_{data} \,|\, L_{\phi_{loc}} \,|\, com_{inc} \,|\, region \,|\, Sig_s \,|\, PU_s \,|\, Sig_b \,|\, PU_b\right]$$

PrivChain

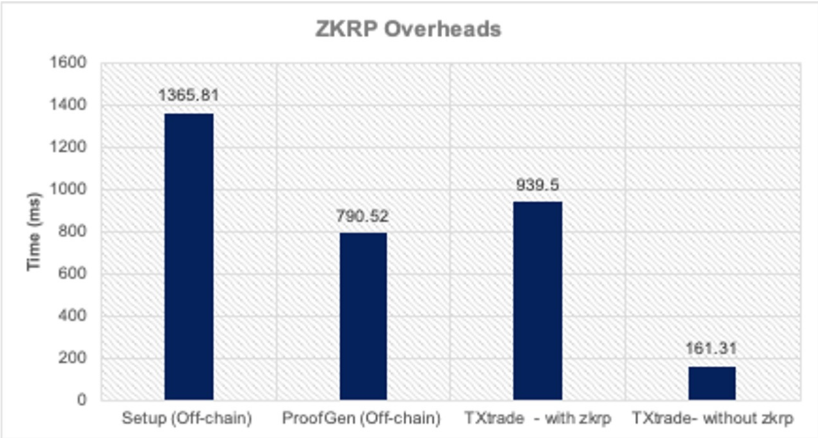
Trade Flow Protection

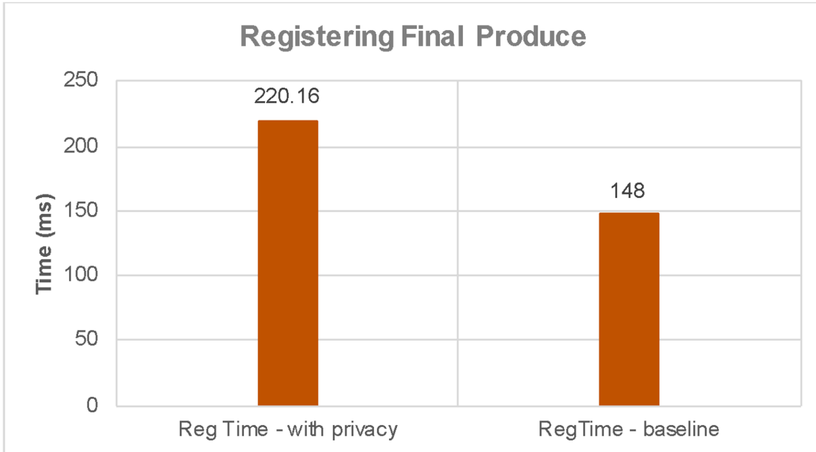
- The provenance of a final product:
  finding the origin of each ingredient using a $TX_{produce}$

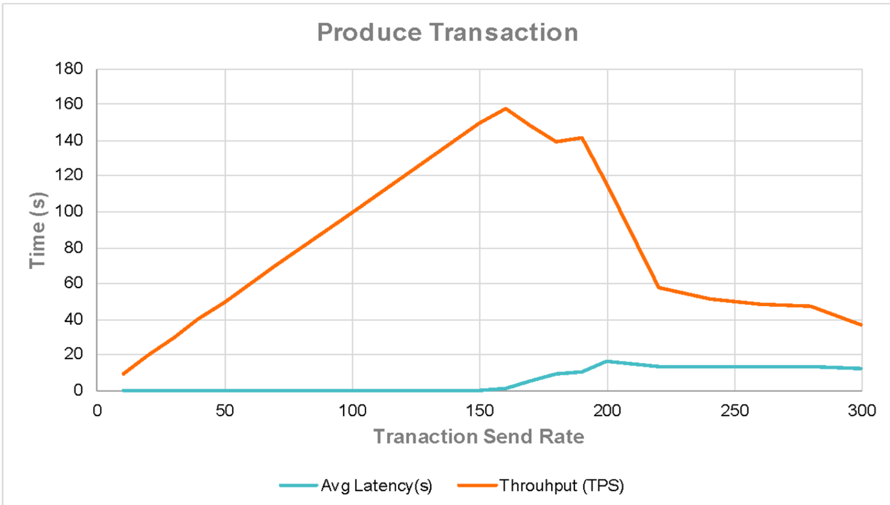
$$TX_{produce} = [ID_{FP} | Enc((ID_{g1}, ..., ID_{gn}), Key) | [regions] | Sig_{buy}]$$

PrivChain

Evaluations







Identity

Permissioned Blockchain

↓

Identities →

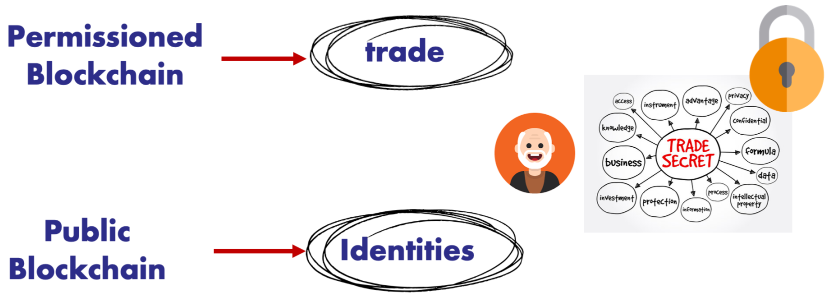
Identity

Permissioned Blockchain

Identities

TradeChain: Key Contributions

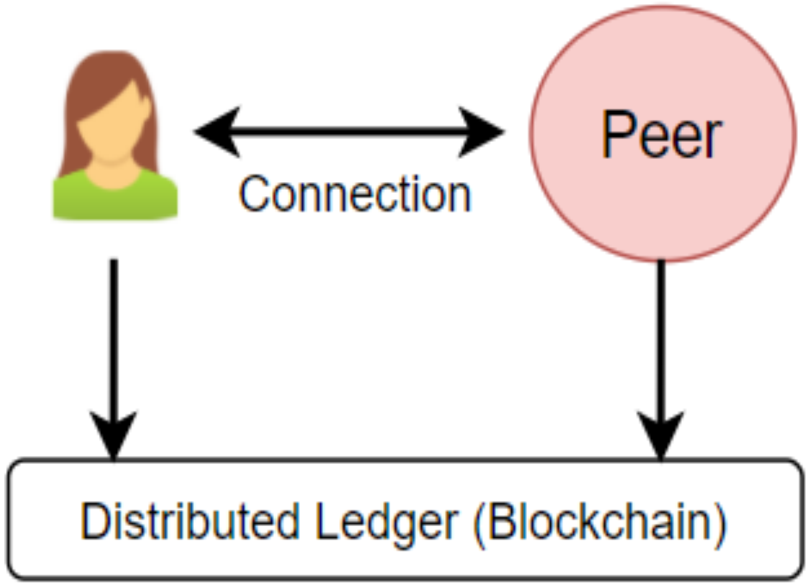
- integrated framework for **two separate ledgers**:
  - IDML for decentralised identity management and
  - TML for recording trade events on the ledger
- supply chain entities can
  - use **ZKPs on their credentials** while trading on TML
  - define **dynamic access rules** for traceability and data collation
- A PoC implementation on **Hyperledger Indy and Fabric** to demonstrate efficacy and minimal overheads



S. Malik, N. Gupta, V. Dedeoglu, S. S. Kanhere and R. Jurdak, TradeChain: Decoupling Traceability and Identity in Blockchain enabled Supply Chains, in Proceedings of TrustCom, virtual, 2021.

Decentralisation of Identity Management

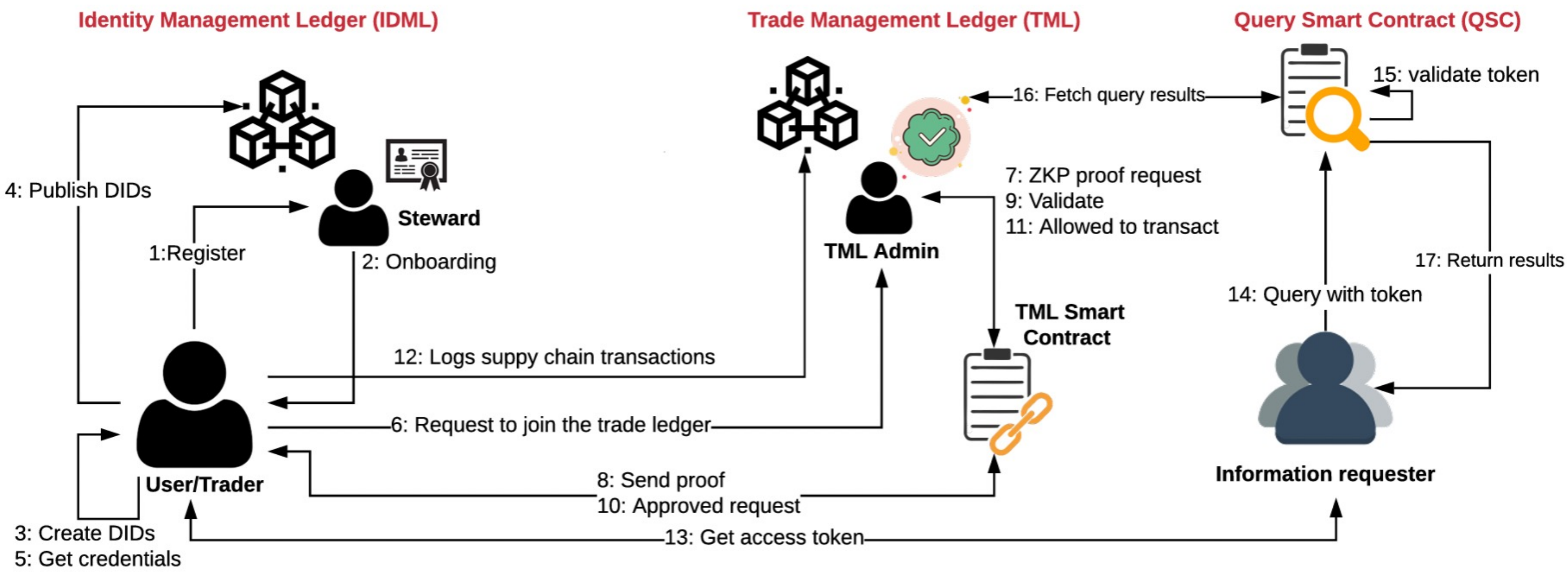
Decentralised, “trustless” ID Provider



- The peer-to-peer relationship secured by public/private key cryptography
- Decentralised registry that verifies the relationships
- Returning people to direct, private connections
- “Me (user)” centric

Self-Sovereign Identity (SSI)

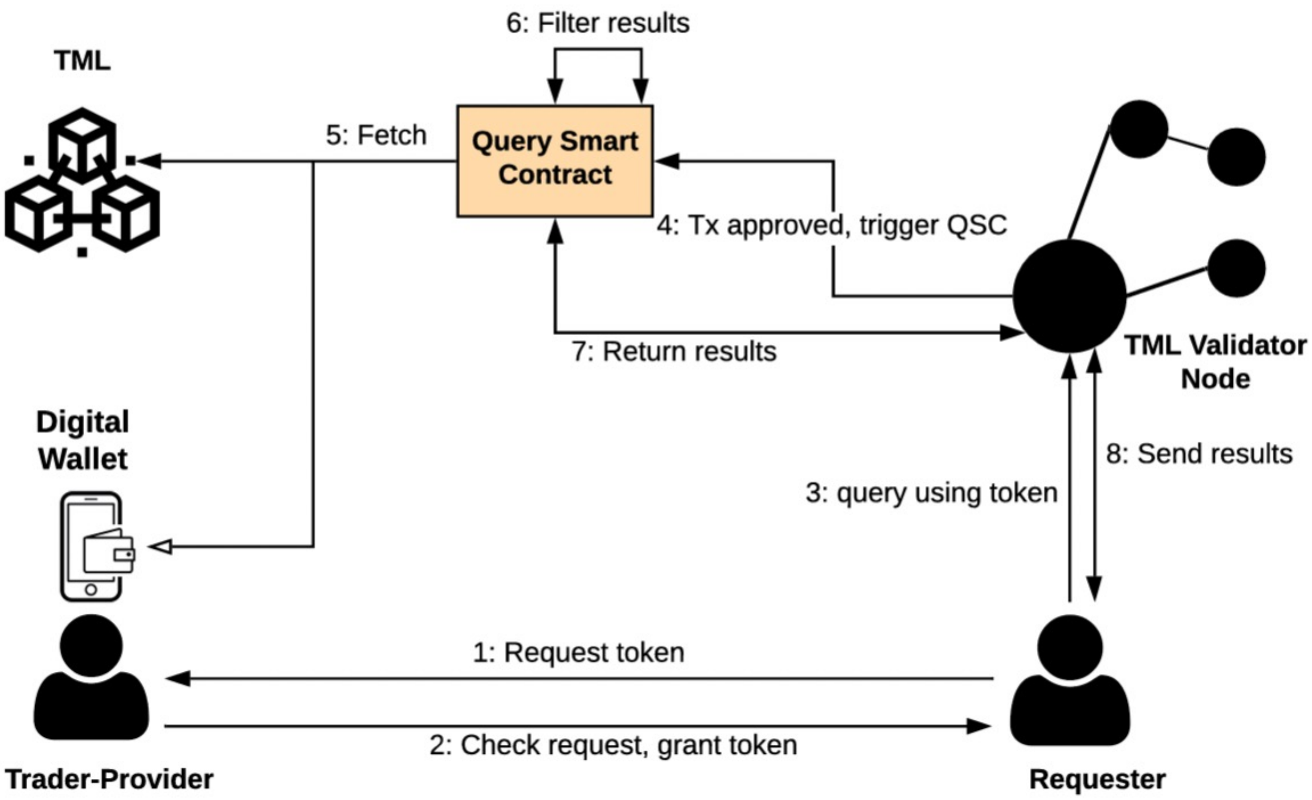
TradeChain
Detailed Framework



UNSW SYDNEY

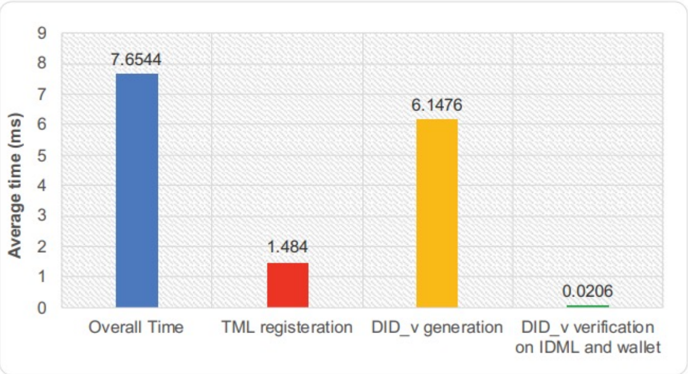
TradeChain

Token-based Querying

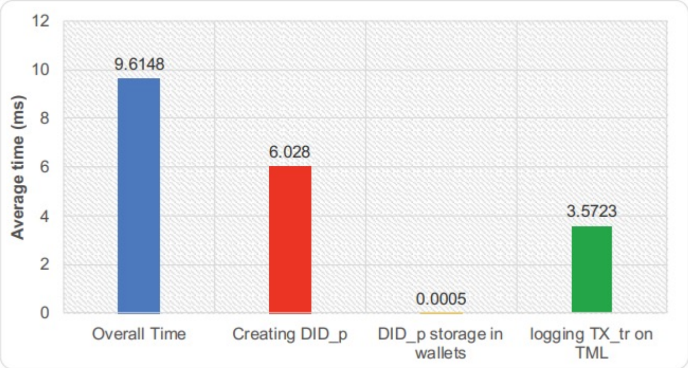


TradeChain

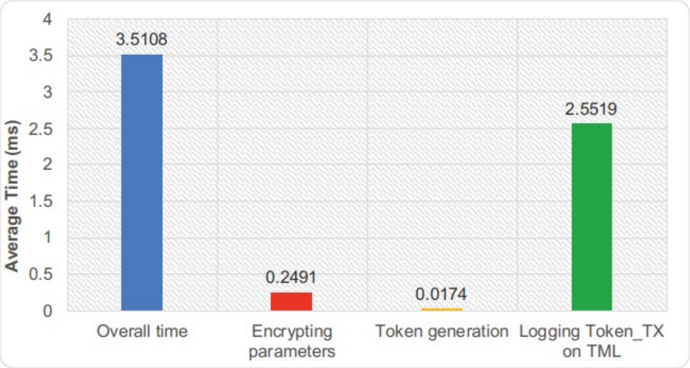
Evaluations



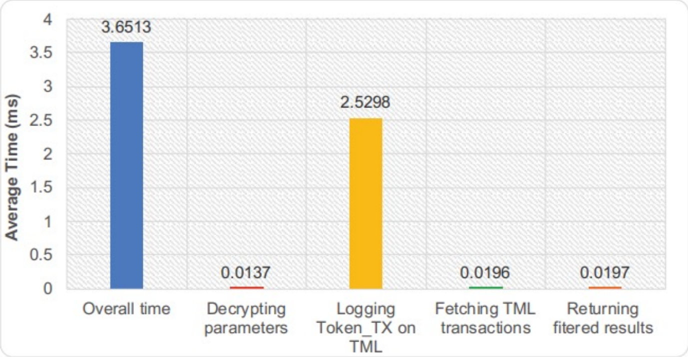
(a) Trader's Registration on TML



(b) Trading a Commodity



(c) Generating a token trading a commodity



(d) Validate token and return results

Time Overheads

Future Opportunities

- Interoperability
  - need to design protocols and standards to develop an interoperability architecture among the **growing parallel solutions**
  - Various interoperability approaches can be adopted such as **APIs and gateways, pub-sub models, notaries, smart contracts,** etc.
- Ascertaining trust
  - Reputation modules are not the only option!
  - Other solutions such as incorporating **smart biological fingerprints** have still not been fully explored
- Incentives
  - Mechanisms **to incentivise** famers/small-scale suppliers need to be designed
  - **Smart contracts** for actioning incentives

Future Opportunities

- Governance
  - some central monitoring or **governance is required for regulatory purposes**
  - need to devise a **governance framework** which allows some level of **autonomy**, but at the same time, can assist the government bodies with having an **oversight over the trade activities**
- Sustainability
  - Quantifying the **carbon footprint** of complex supply chains is necessary
  - Mechanisms to check if **sustainability practices** were adopted
  - Improving working/living conditions of farmers

UNSW SYDNEY

E: salil.kanhere@unsw.edu.au

www.linkedin.com/in/salilkanhere