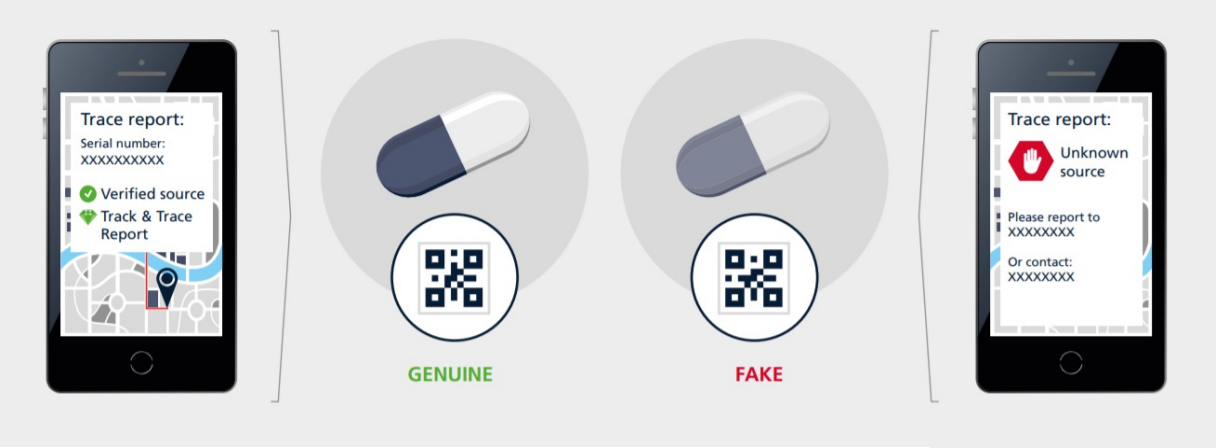
Human-centered and Verifiable Blockchain-based Systems for Trusted Multi-stakeholder Applications

Gowri Sankar Ramachandran

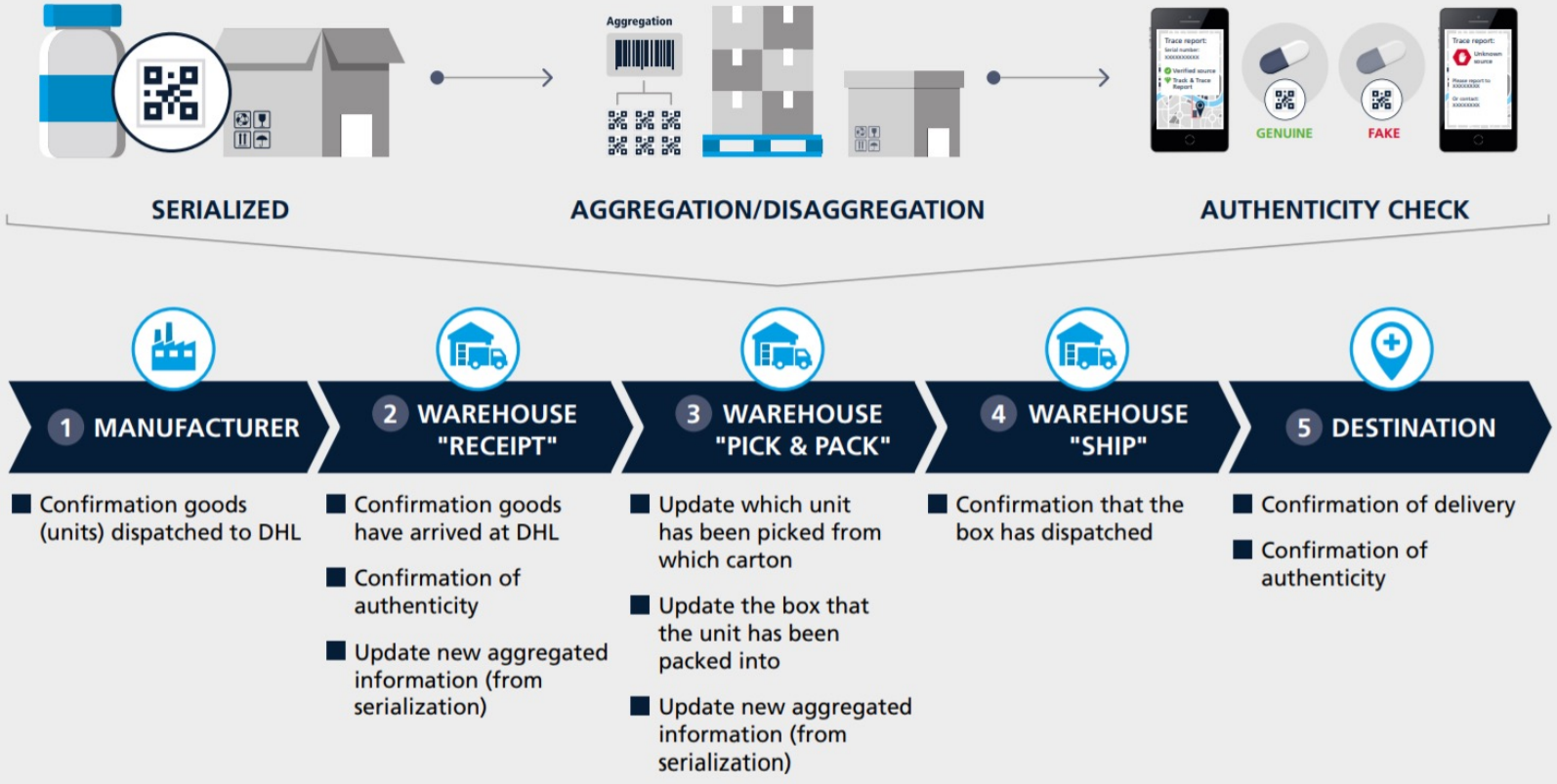
Research Fellow in Distributed Systems, Blockchain and Internet of Things

Trusted Networks Lab,
School of Computer Science, Faculty of Science,
Queensland University of Technology

SDLT 2021, Brisbane



Identifying fake medications through tracking

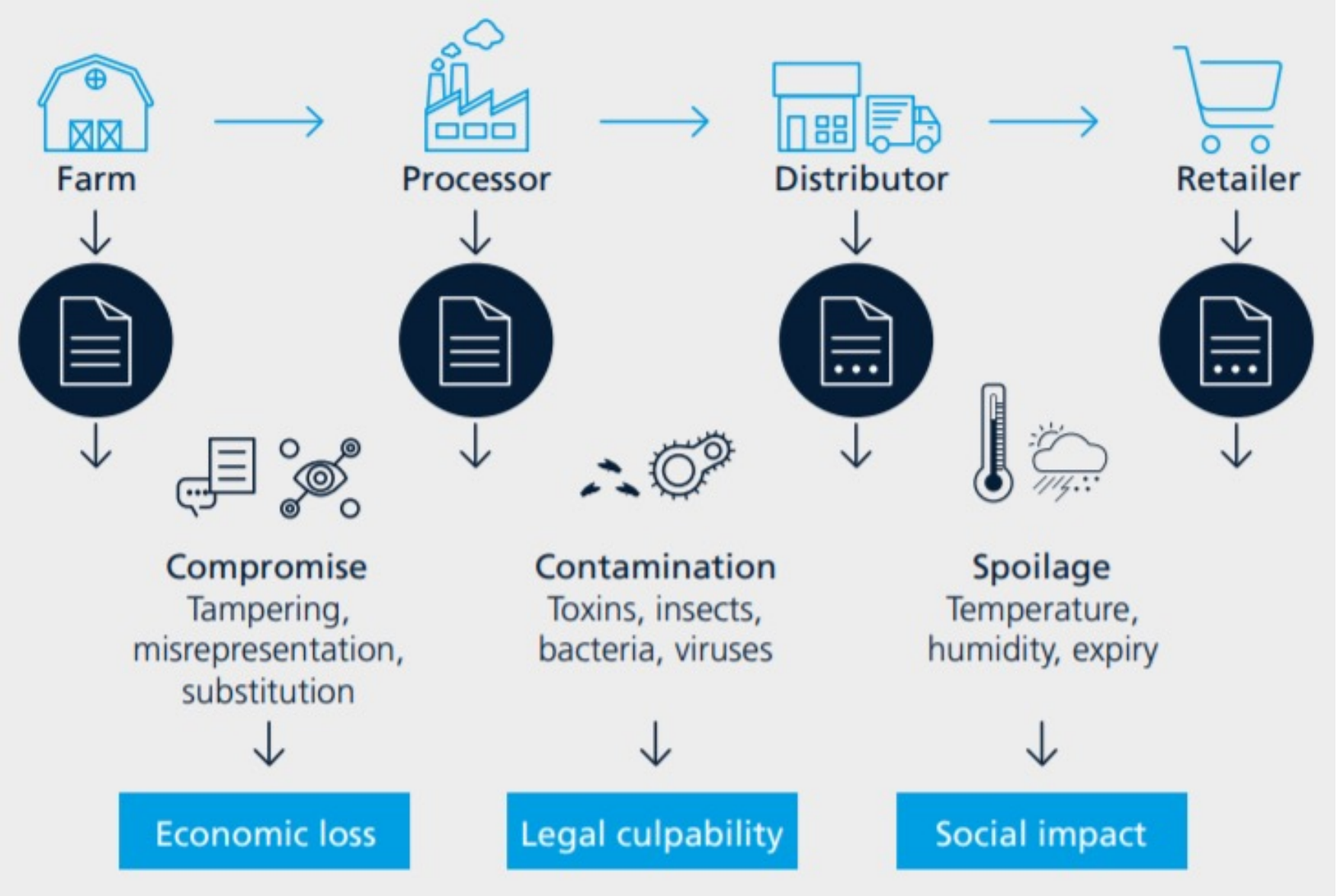


Source:
https://techwireasia.com/2018/03/can-blockchain-kill-counterfeit-pill/

Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

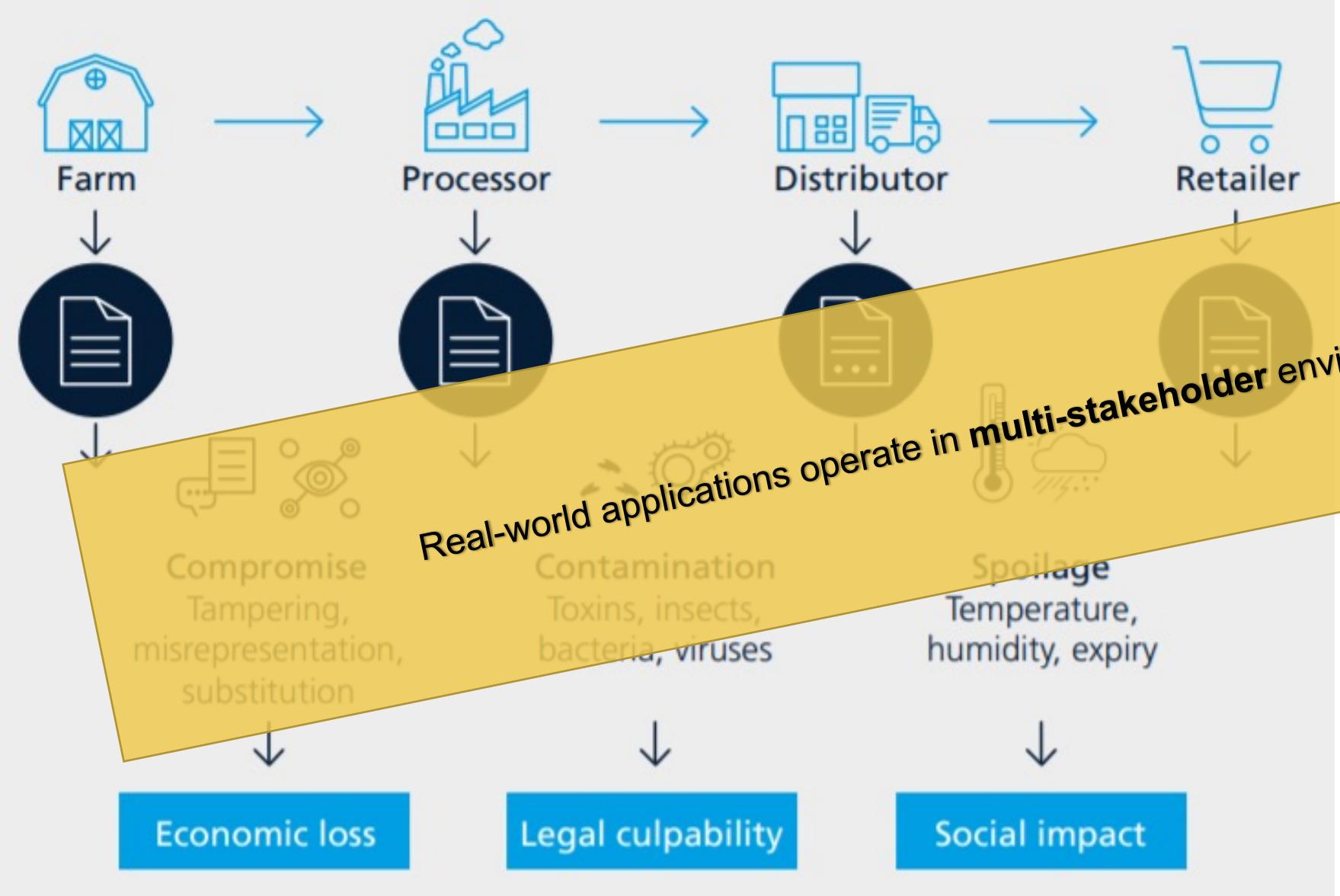
TruNets Trusted Networks Lab

QUT



Source: IBM

Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.



Real-world applications operate in **multi-stakeholder** environments

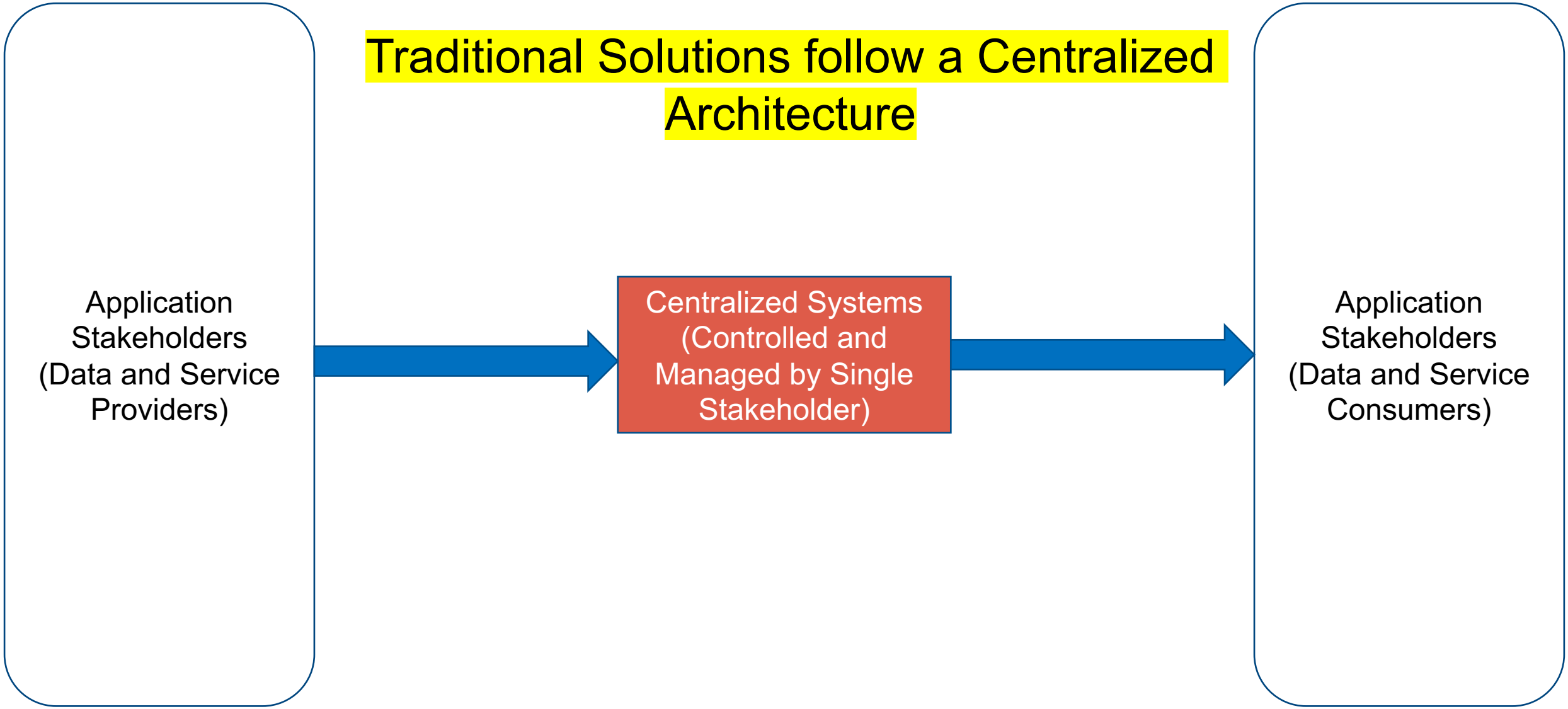
Source: IBM

Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

TruNets Trusted Networks Lab

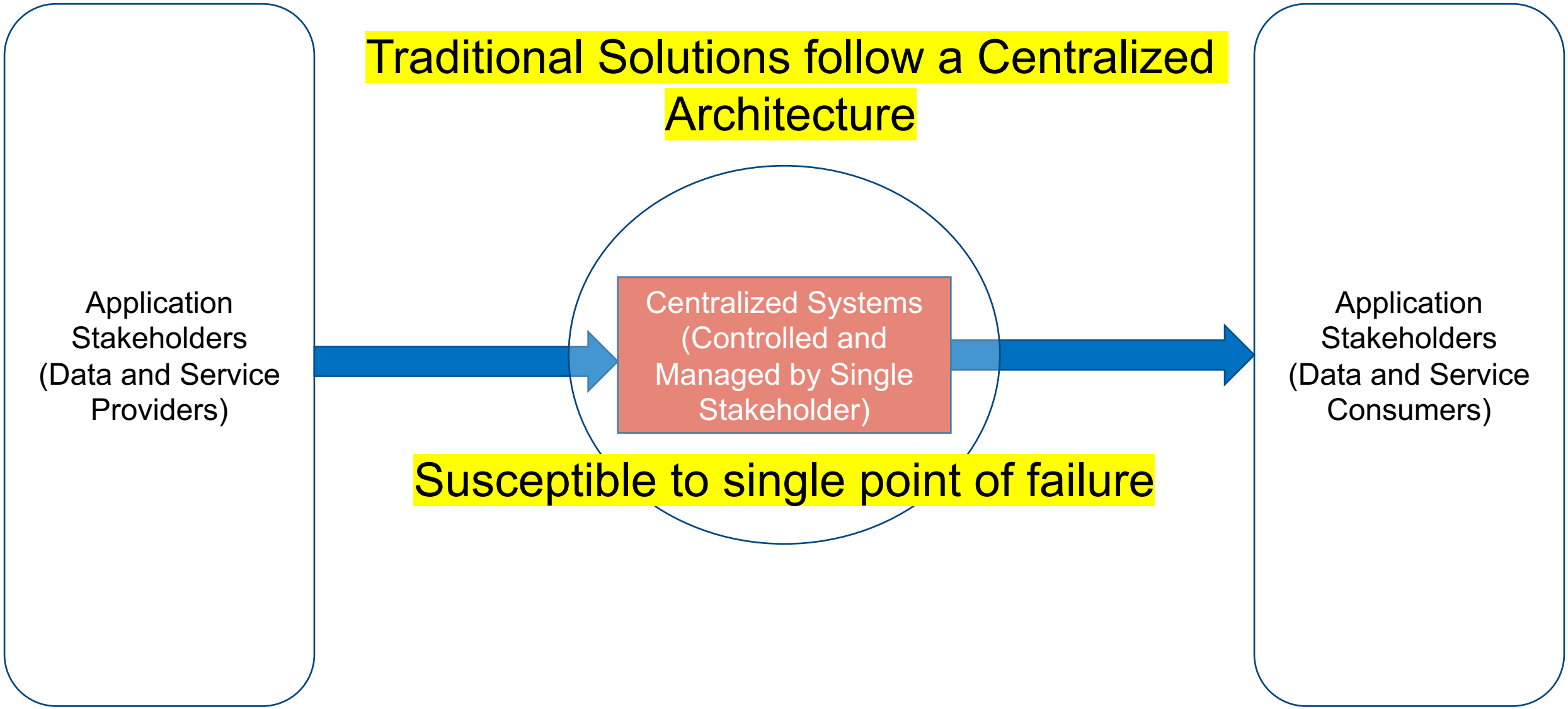
QUT

Traditional Solutions follow a Centralized Architecture



Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

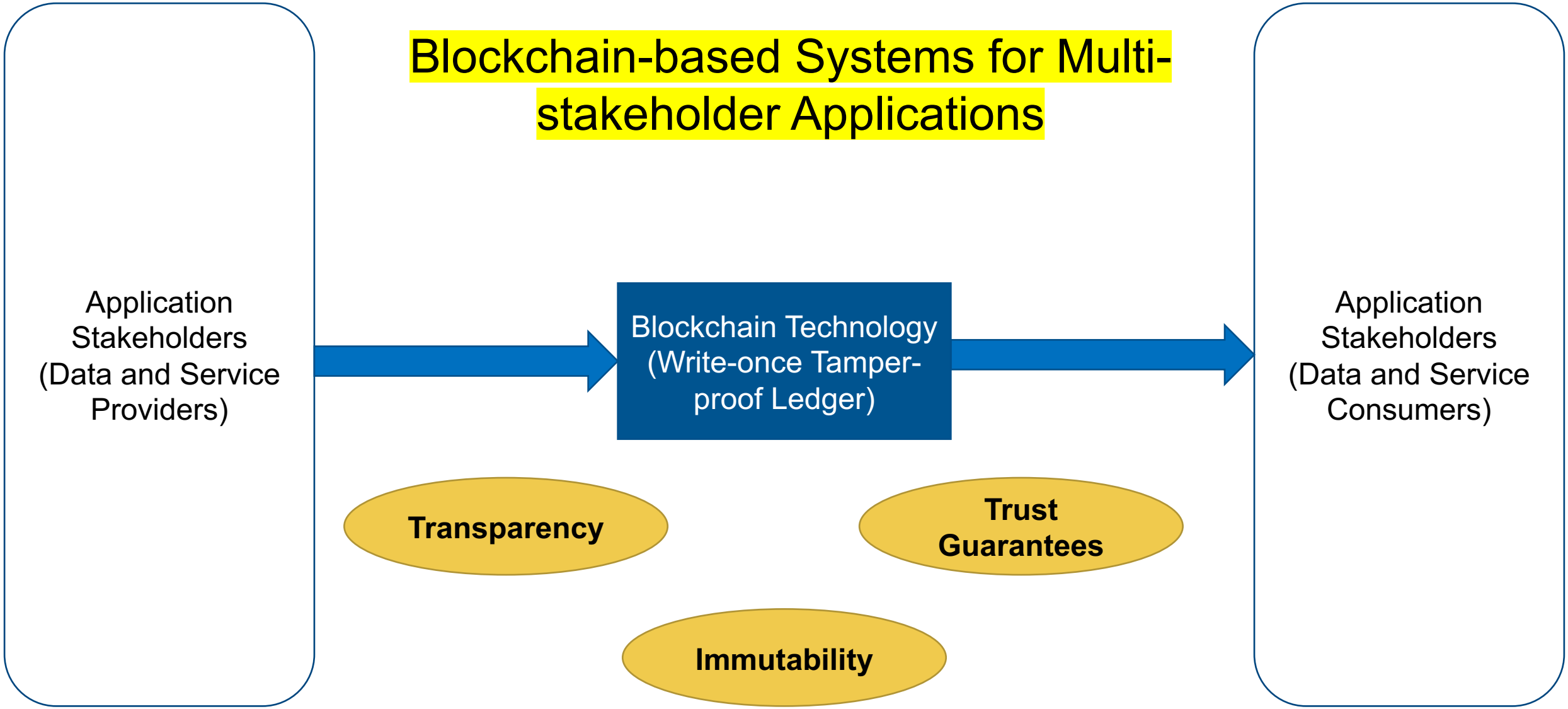
Traditional Solutions follow a Centralized Architecture



Susceptible to single point of failure

Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

Blockchain-based Systems for Multi-stakeholder Applications

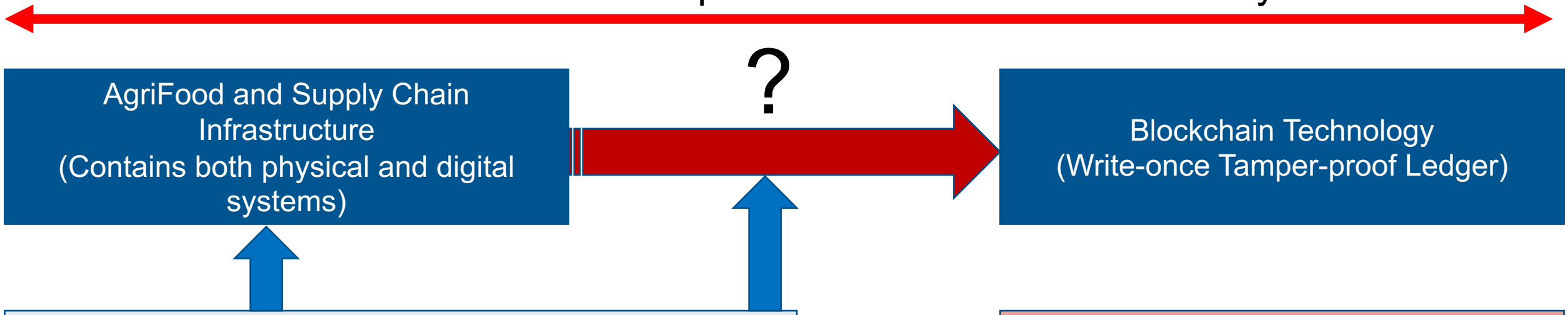


Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

TruNets Trusted Networks Lab

QUT

End-to-End Trust Requires Trusted Methods at All Layers



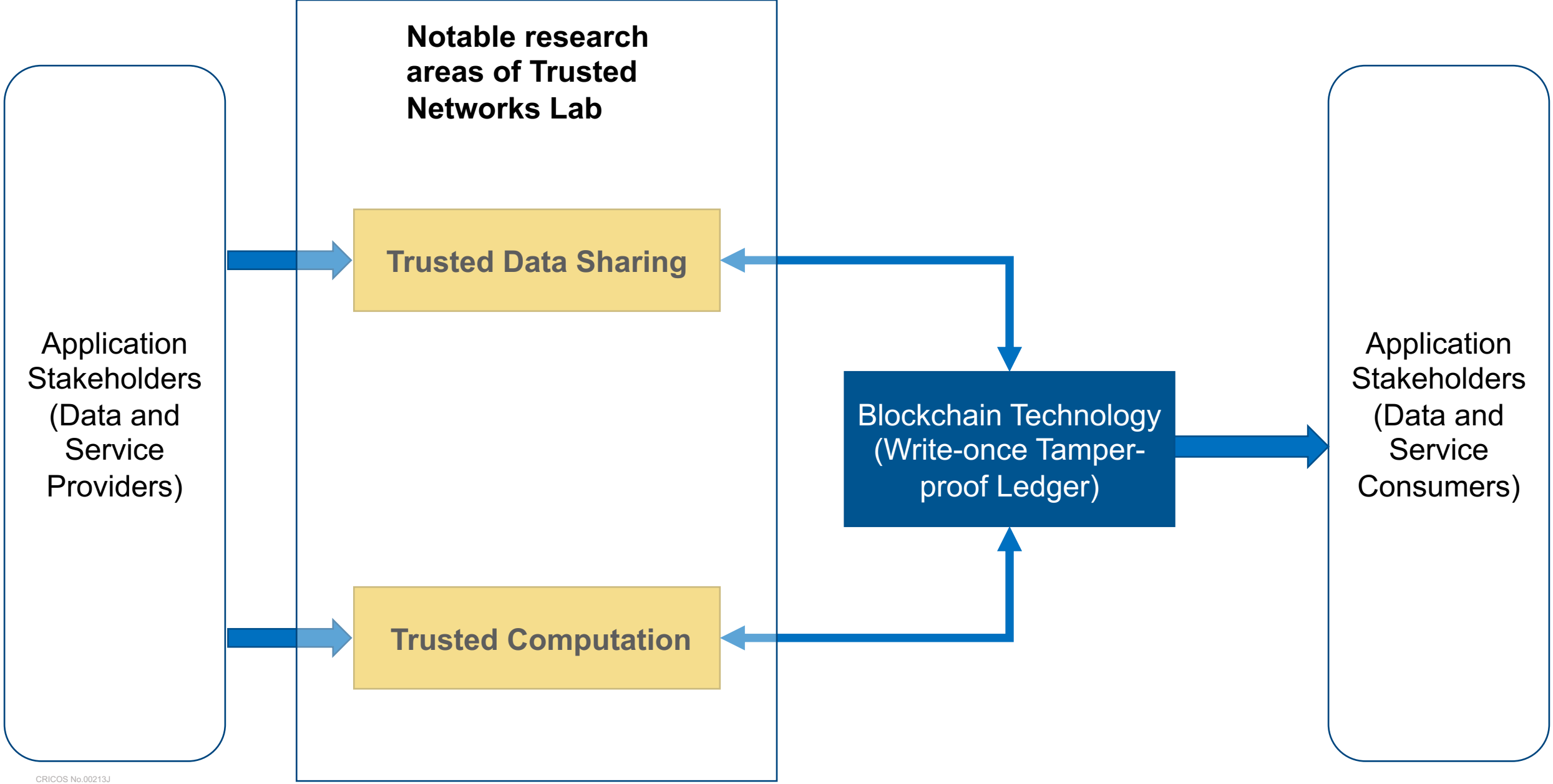
- Blockchain **stores information in a tamper-proof ledger** through a trusted consensus process
- Blockchain lacks intelligence to **verify the credibility of the information**
  - This problem is known as **"Garbage-In-Garbage-Out"** problem
- **Important and Open Problem** in the design and adoption of multi-stakeholder blockchain-based systems
  - Develop trusted processes to translate data from physical to digital world

- Blockchain technology can **guarantee trust provided the information it receives from the other systems are authentic and verifiable**

Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

TruNets Trusted Networks Lab

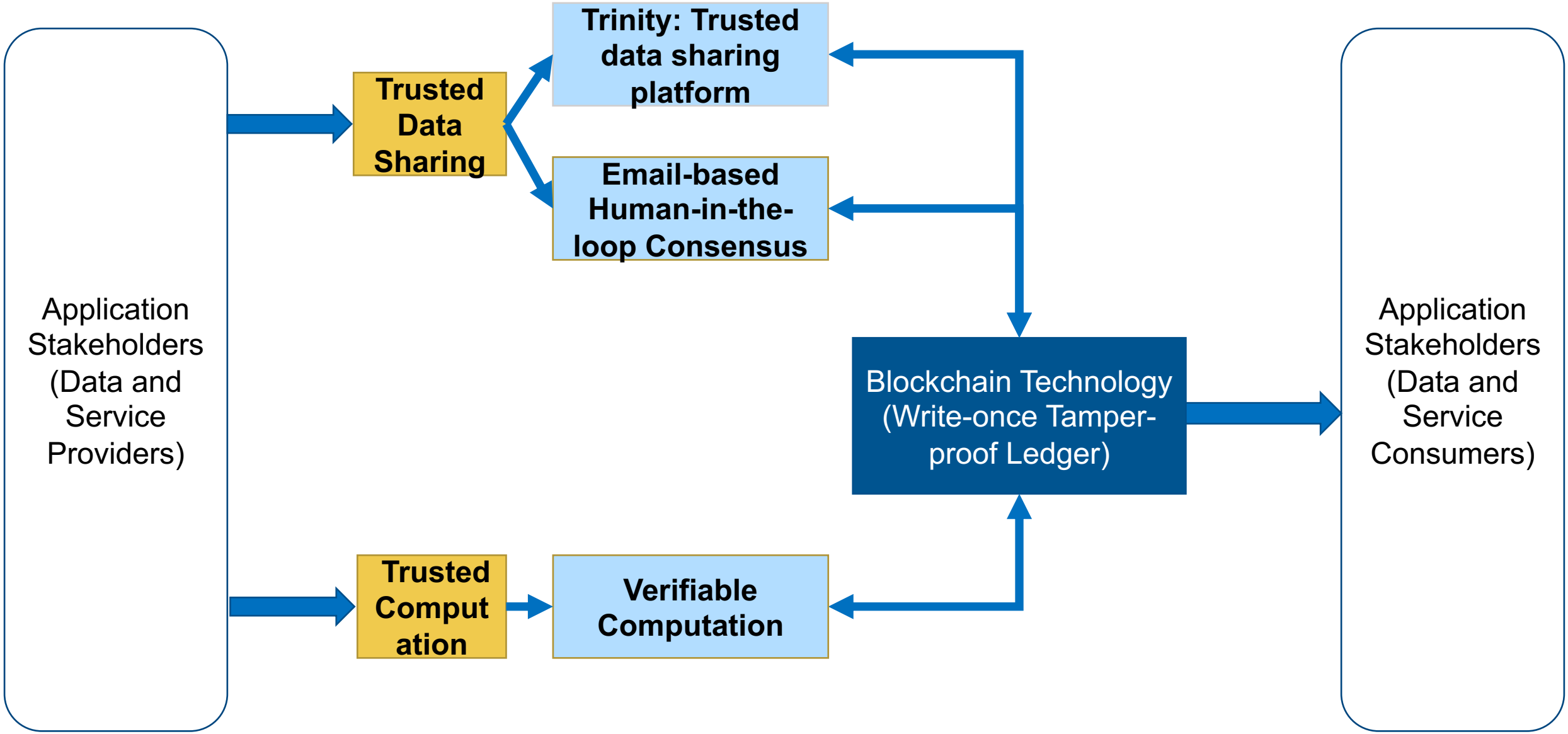
QUT



Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

TruNets Trusted Networks Lab

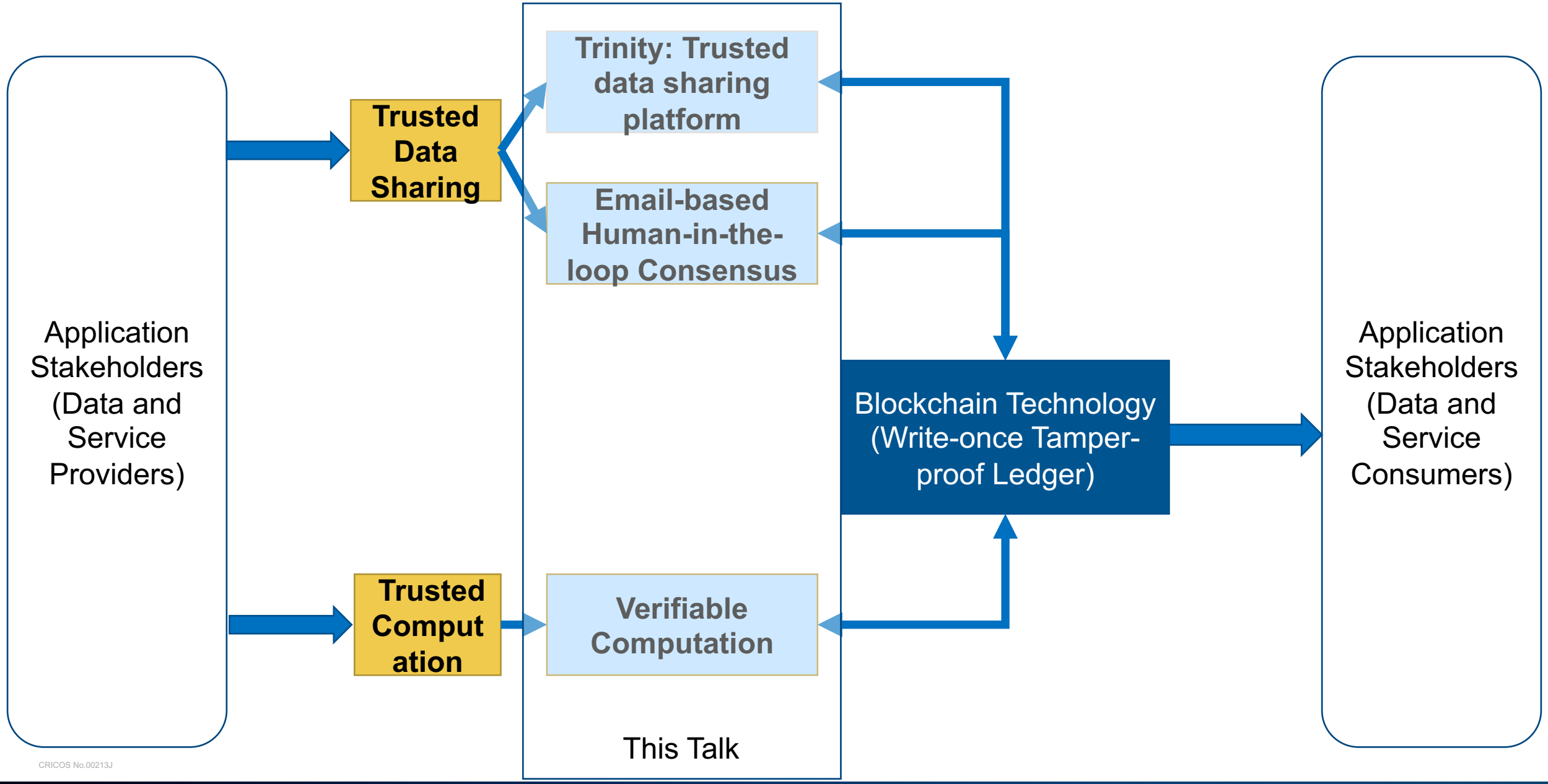
QUT



Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

TruNets Trusted Networks Lab

QUT



Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

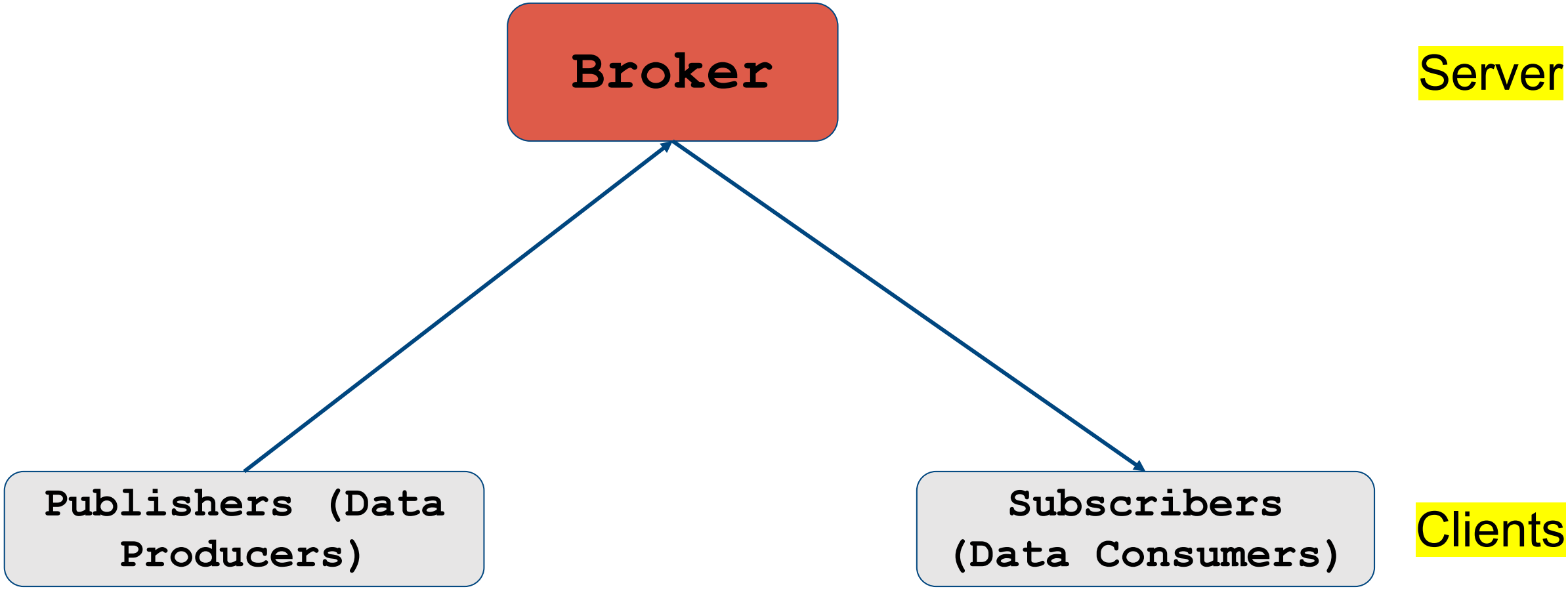
TruNets Trusted Networks Lab

QUT

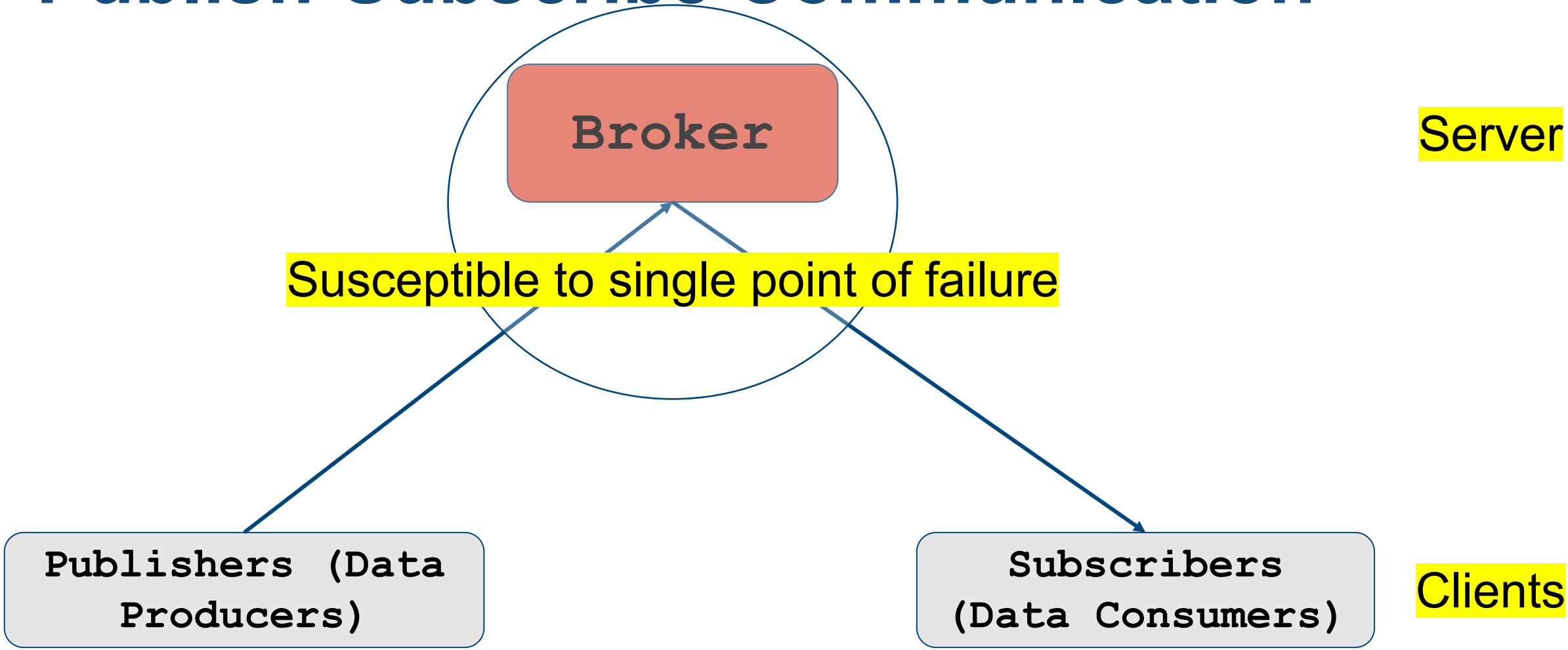
Trusted Data Sharing using Trinity

G. S. Ramachandran et al., "Trinity: A Byzantine Fault-Tolerant Distributed Publish-Subscribe System with Immutable Blockchain-based Persistence," **2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)**, 2019, pp. 227-235, doi: 10.1109/BLOC.2019.8751388.

Publish-Subscribe Communication

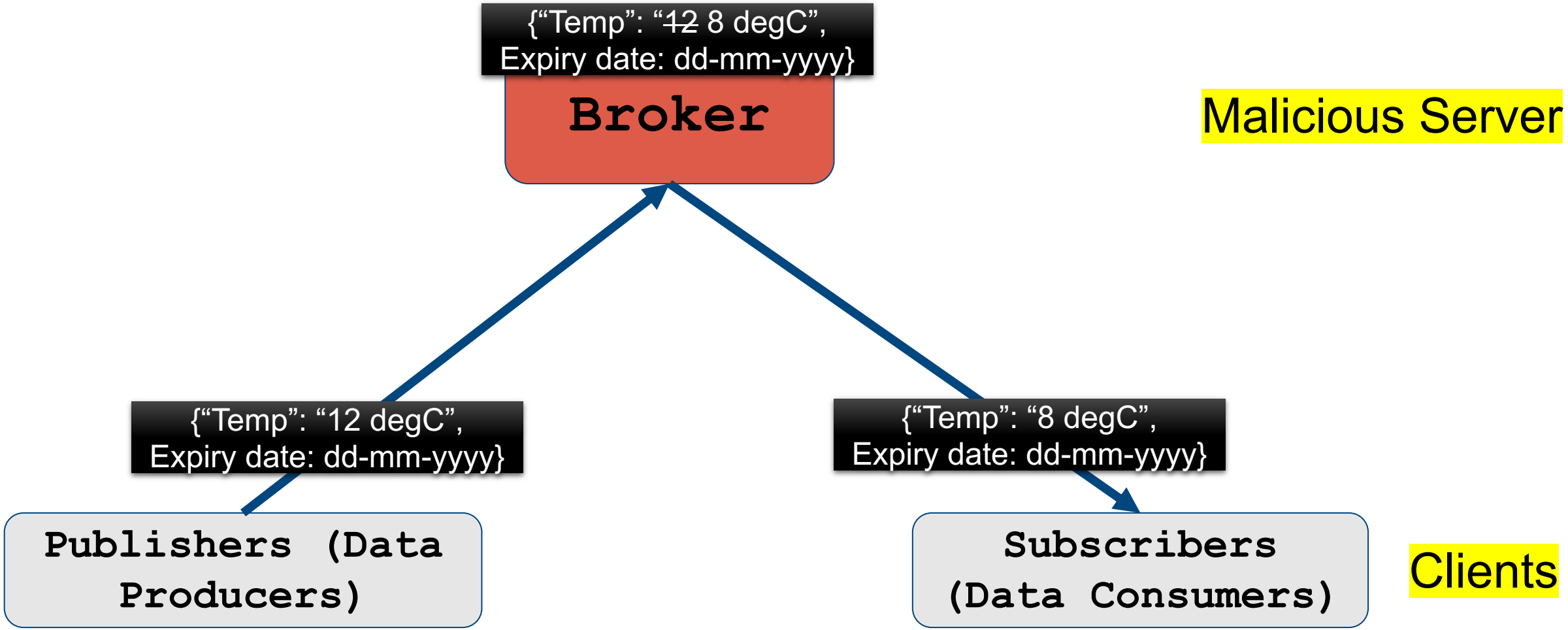


Publish-Subscribe Communication



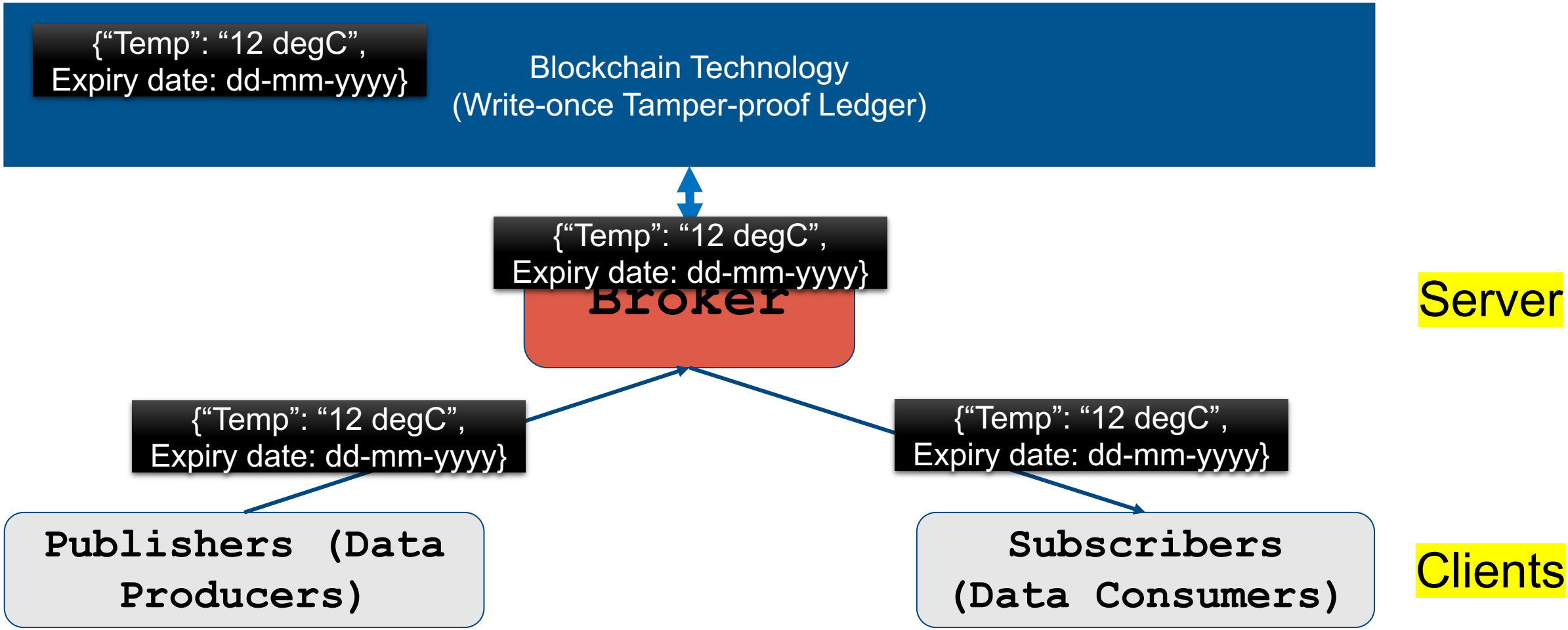
Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

Publish-Subscribe Communication



Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

Trinity: Distributed Publish-Subscribe Framework

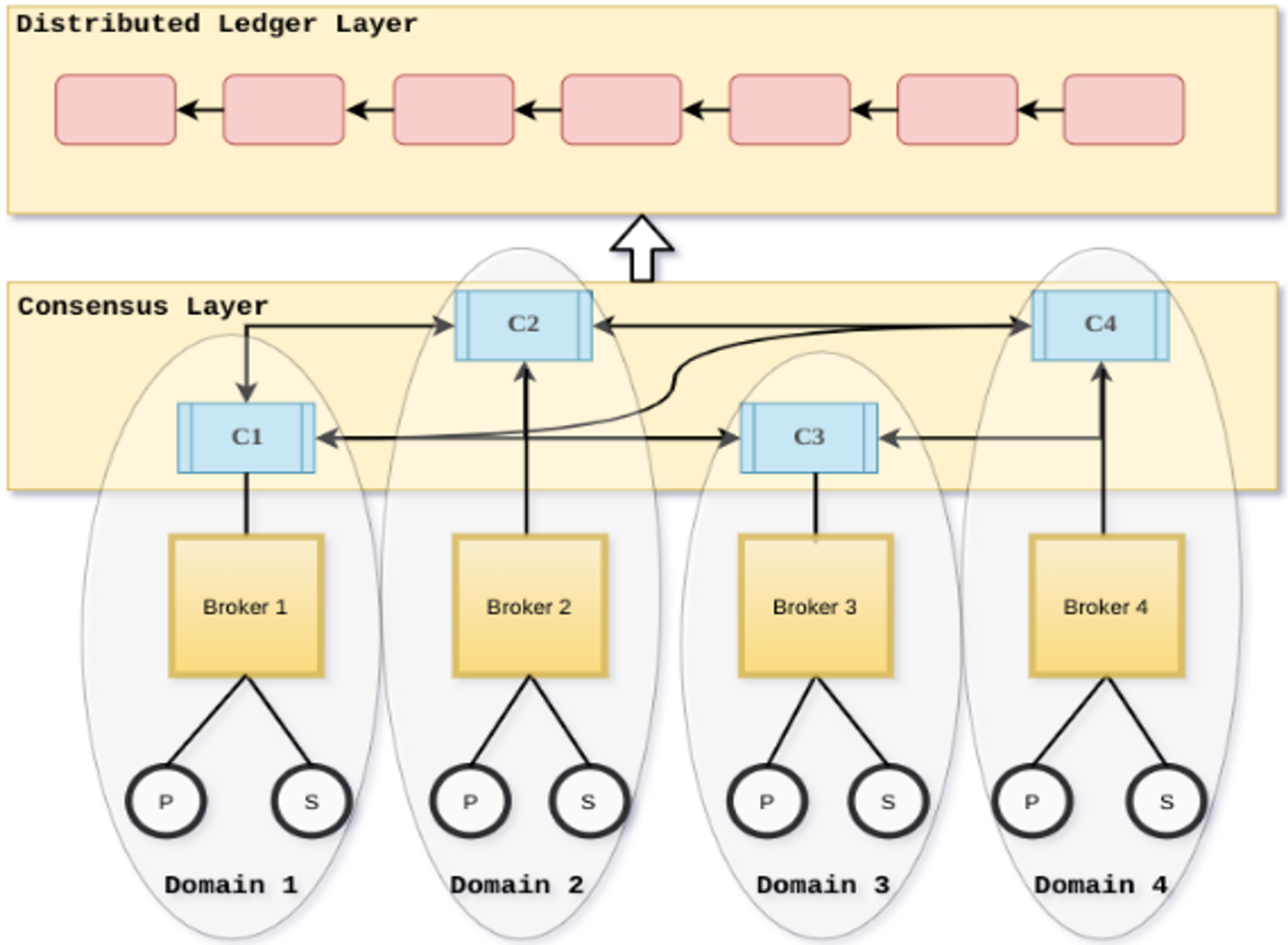


Publishers and subscribers can verify the data integrity by checking the public ledger.

Trinity is ideal for trusted data sharing

- For more information, please refer to the following article: G. S. Ramachandran *et al*., "Trinity: A Byzantine Fault-Tolerant Distributed Publish-Subscribe System with Immutable Blockchain-based Persistence," *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2019, pp. 227-235, doi: 10.1109/BLOC.2019.8751388.

- Open-source Software: **https://github.com/ANRGUSC/Trinity**



CRICOS No.00213J

Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

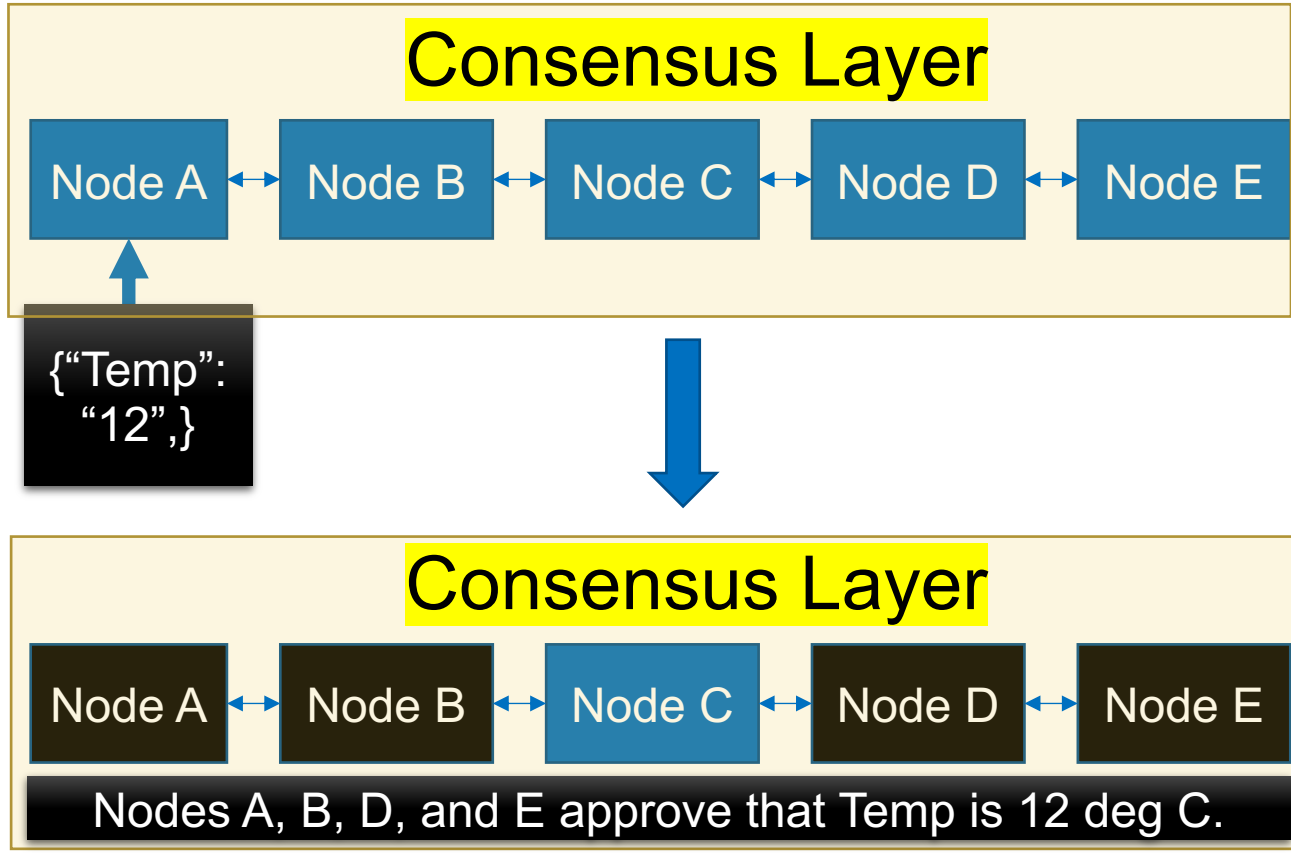
TruNets Trusted Networks Lab

Email-based Human-centered Consensus for Multi-stakeholder Applications

Ongoing Work

Blockchain Consensus in a Nutshell

- Consensus algorithms help nodes to agree on the state of the system
- Byzantine fault-tolerant consensus is one of the popular algorithms
  - System state (or transaction) must be approved by more than two-thirds of the nodes in the network
- Approval process lacks intelligence
  - Rule-based approval without human inputs

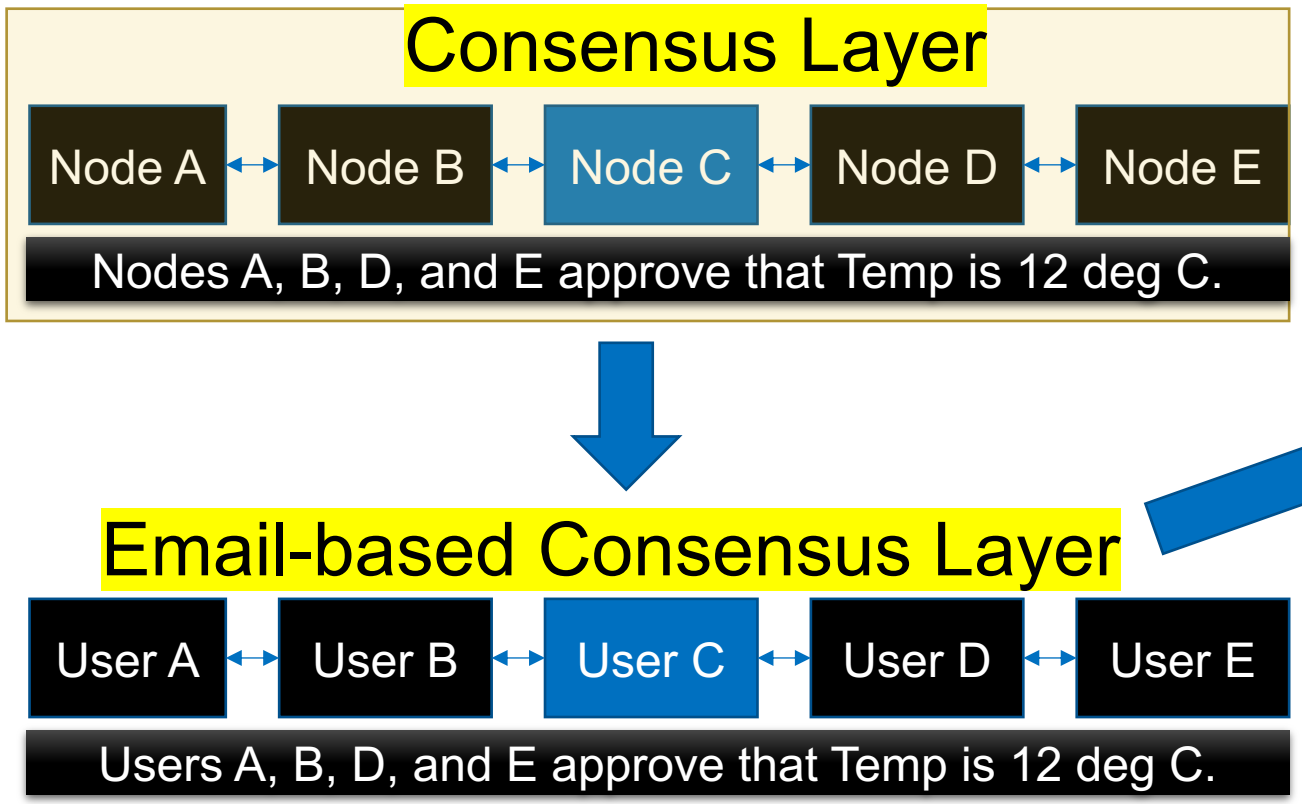


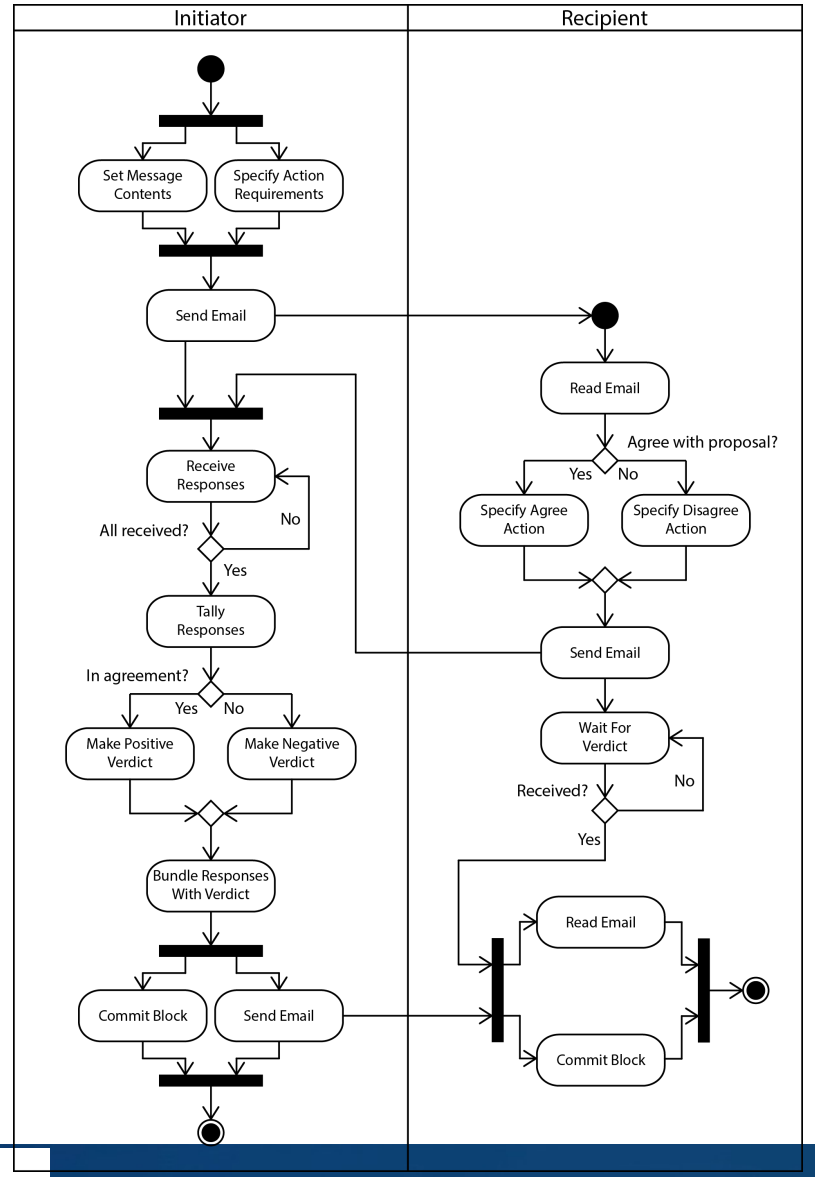
Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

TruNets Trusted Networks Lab

QUT

Towards Human-centered Consensus





CRICOS No.00213J

Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

TruNets Trusted Networks Lab

QUT

Benefits of Human-centered Consensus

- Some business transactions cannot be automated with rules - domain experts may have to weigh in
  - Example: Compliance management in supply chain
- Risky business transactions require human oversight
  - Example: Payment clearance in a supply chain

- Human centered consensus allows
  - Business managers and key stakeholders to involve in the decision making process
  - Maintains a record of interactions, including approvals, in immutable blockchain ledger

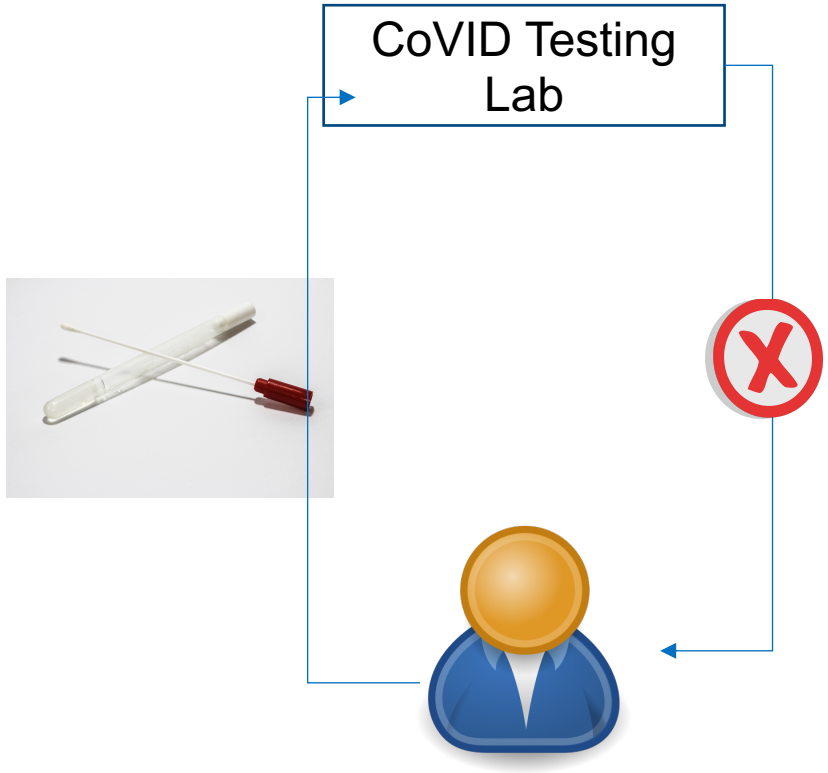
Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

Verifiable Computation for Business Processes

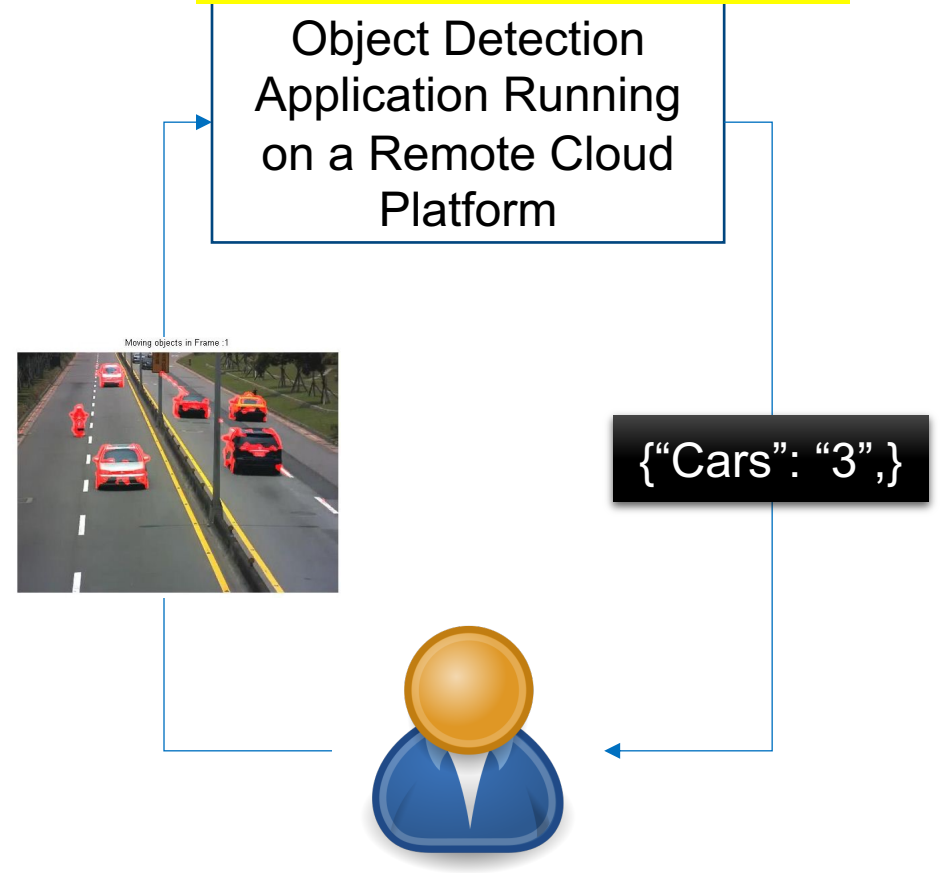
Ongoing Work

Why Verifiable Computation?

Can you be sure that the lab analyzed your results?



Can you be sure that the remote computer correctly executed the code?



CRICOS No.00213J

Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

TruNets Trusted Networks Lab

QUT

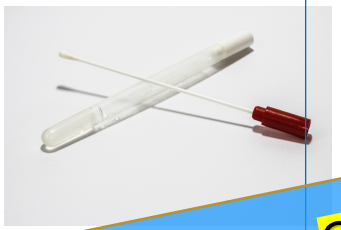
Why Verifiable Computation?

Can you be sure that the lab analyzed your results?

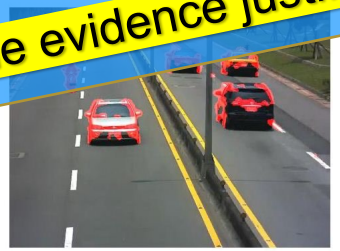
Can you be sure that the remote computer correctly executed the code?

CoVID Testing Lab

Object Detection Application Running on a Remote Cloud Platform



Can we ask remote computation platforms to provide evidence justifying correctness?



{“Cars”: “3”,}

CRICOS No.00213J

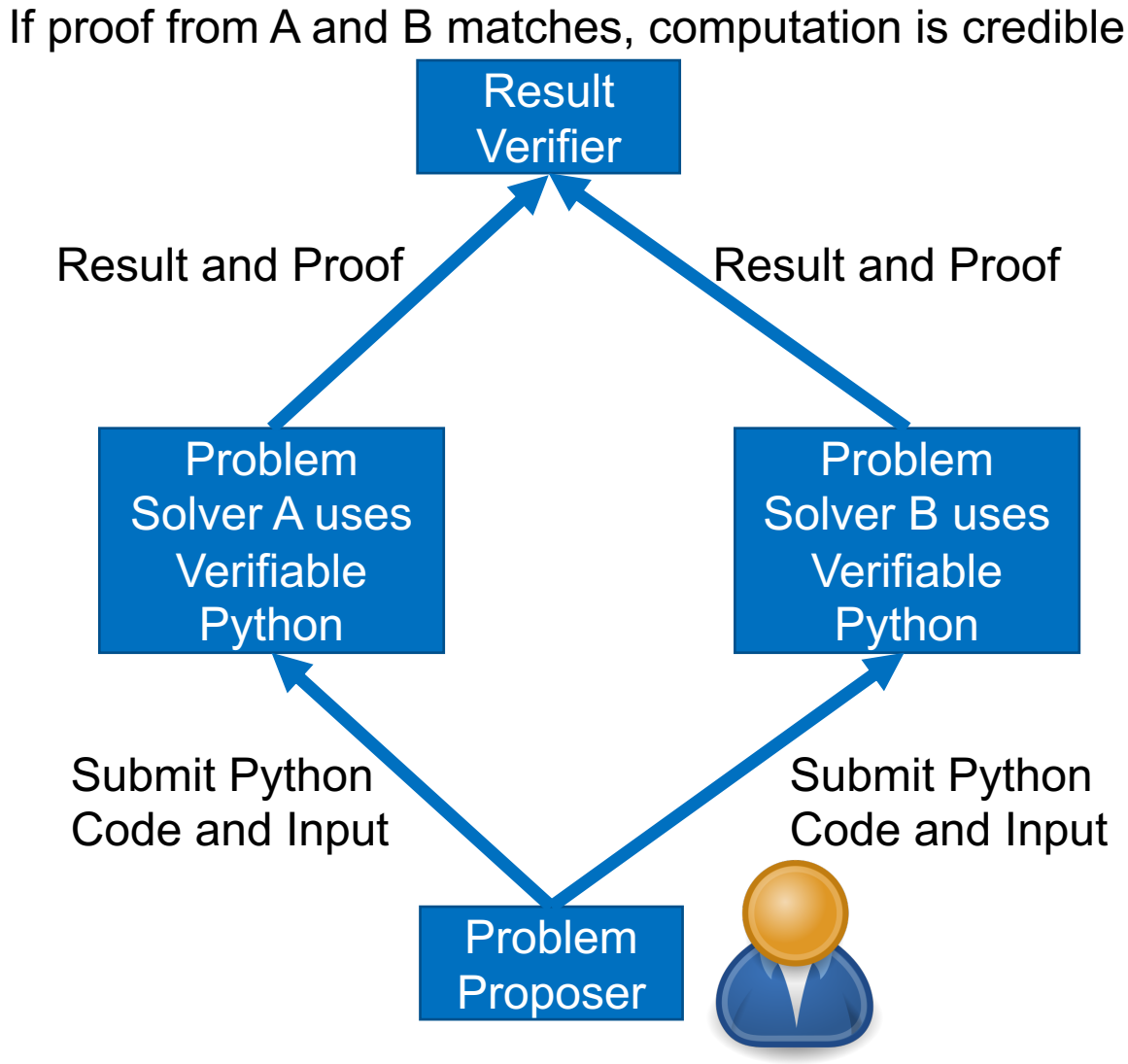
Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

TruNets Trusted Networks Lab

QUT

Verifiable Python

- Verifiable Python (vPython) is an extended version of Python, which generates proof for Python applications
- vPython generates runtime traces in the background when the Python interpreter executes the code
- Runtime traces provide detailed information about the execution of the code



Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

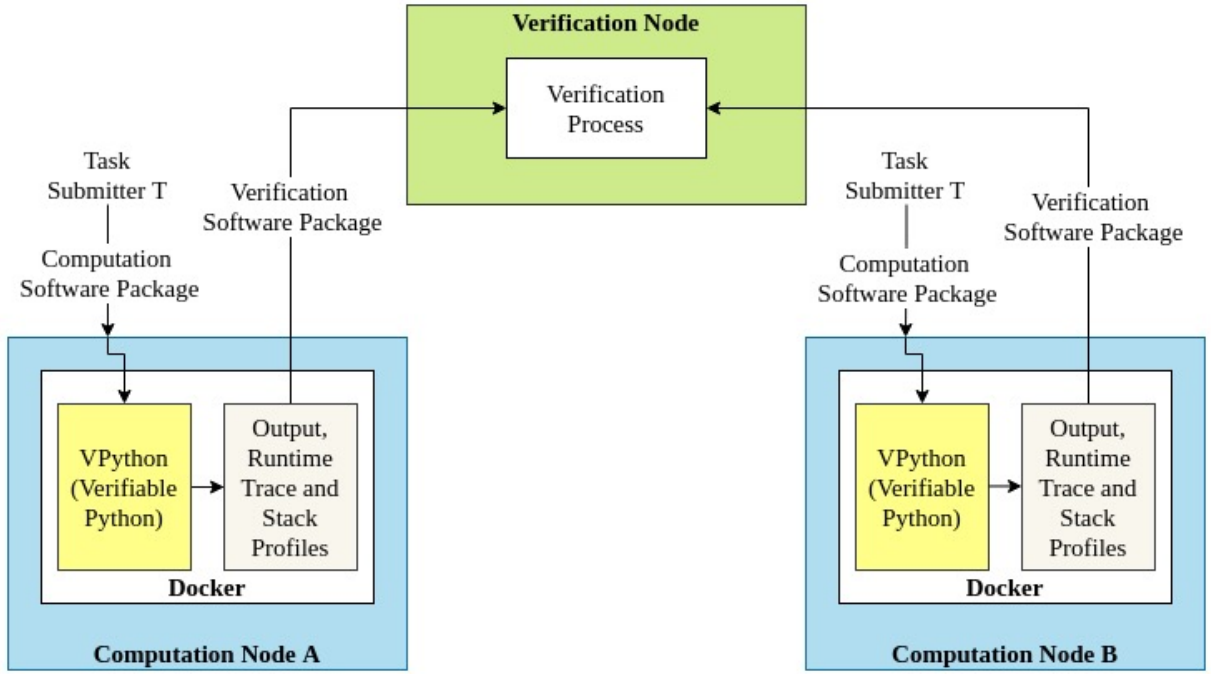
TruNets Trusted Networks Lab

QUT

vPython for Verifiable Computation

- Ramachandran, G., Nemeth, D., Neville, D., Zhelezov, D., Yalçin, A., Fohrmann, O., & Krishnamachari, B. (2020, November). WhistleBlower: Towards A Decentralized and Open Platform for Spotting Fake News. In 2020 IEEE International Conference on Blockchain (Blockchain) (pp. 154-161). IEEE.

- https://github.com/ANRGUSC/vPython



Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

TruNets Trusted Networks Lab

QUT

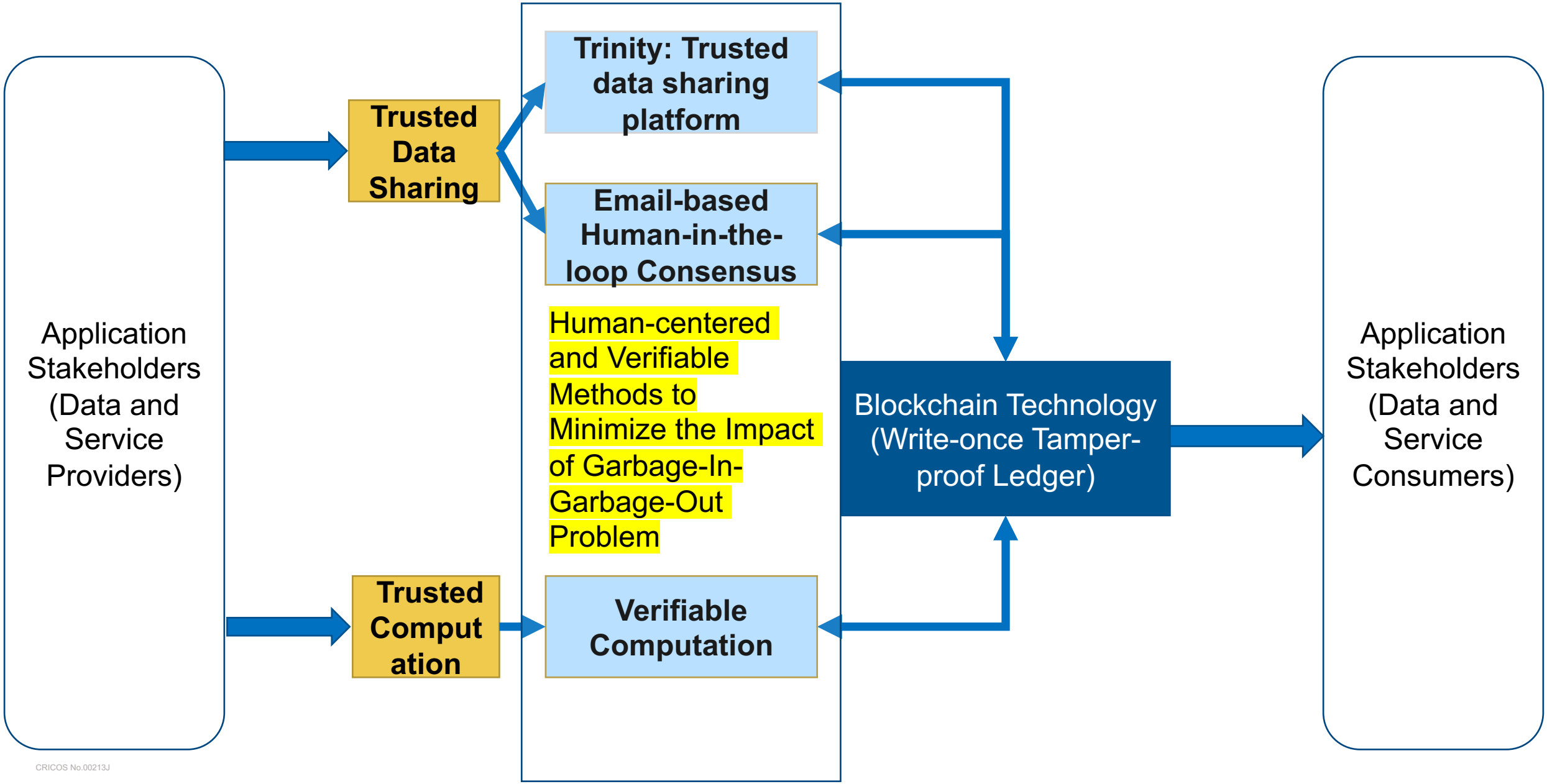
Conclusion

- Multi-stakeholder applications require trusted data sharing and computation platforms
- Centralized solutions suffer from single point of failure
- Blockchain is good but suffer from garbage-in-garbage-out problem
- Trinity: a trusted data sharing framework based on blockchain
  - Offers transparency and immutability
- Human-centered consensus based on email
  - Brings human to the decision-making process – enabling verifiability through an immutable ledger and a trusted protocol
- Verifiable computation helps users perform computation reliably on a remote computer
  - vPython offers a tool to check the computation's credibility

Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

TruNets Trusted Networks Lab

QUT



Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

TruNets Trusted Networks Lab

QUT

Resources

- G. S. Ramachandran *et al*., "Trinity: A Byzantine Fault-Tolerant Distributed Publish-Subscribe System with Immutable Blockchain-based Persistence," *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2019, pp. 227-235, doi: 10.1109/BLOC.2019.8751388.
- Ramachandran, G., Nemeth, D., Neville, D., Zhelezov, D., Yalçin, A., Fohrmann, O., & Krishnamachari, B. (2020, November). WhistleBlower: Towards A Decentralized and Open Platform for Spotting Fake News. In *2020 IEEE International Conference on Blockchain (Blockchain)* (pp. 154-161). IEEE.

Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

Resources

- https://github.com/ANRGUSC/Trinity
- https://github.com/ANRGUSC/vPython

Gowri Sankar Ramachandran (g.ramachandran@qut.edu.au)
Trusted Networks Lab, School of Computer Science, Faculty of Science.

Thanks!

Gowri Sankar Ramachandran
Email: g.ramachandran@qut.edu.au

https://research.qut.edu.au/trustednetworks/