



Blockchain Risks, Opportunities and Future Scenarios

Mark Staples

Research Group Leader – Software Systems

www.csiro.au



AUSTRALIA'S DIGITAL INNOVATION POWERHOUSE

DATA
61



1100⁺

employees
[including students]

415⁺

students

31

Government
partners

91

Corporate
partners

38

University
partners

190⁺

data-driven
projects

172

patents

WE FOCUS ON EVERY ASPECT OF DATA R&D



- 1 Data capture and consumption
- 2 Communications and networking
- 3 Infrastructure
- 4 Hardware and software
- 5 Cybersecurity
- 6 Data statistics, modeling and analytics
- 7 Decision sciences
- 8 Behavioural economics and cognitive sciences

DATA
61



Looking (Back) at Data61 Treasury Projects



- Two concurrent projects, Jul 2016 – May 2017
- Funded via National Innovation Science Agenda
- With help from The Treasury
- Reports available:
<http://www.data61.csiro.au/blockchain>
- Today:
 - What did the projects do, and what did the reports say?
 - What's changed, and what's next?

DISTRIBUTED LEDGERS

Scenarios for the Australian economy
over the coming decades

May 2017



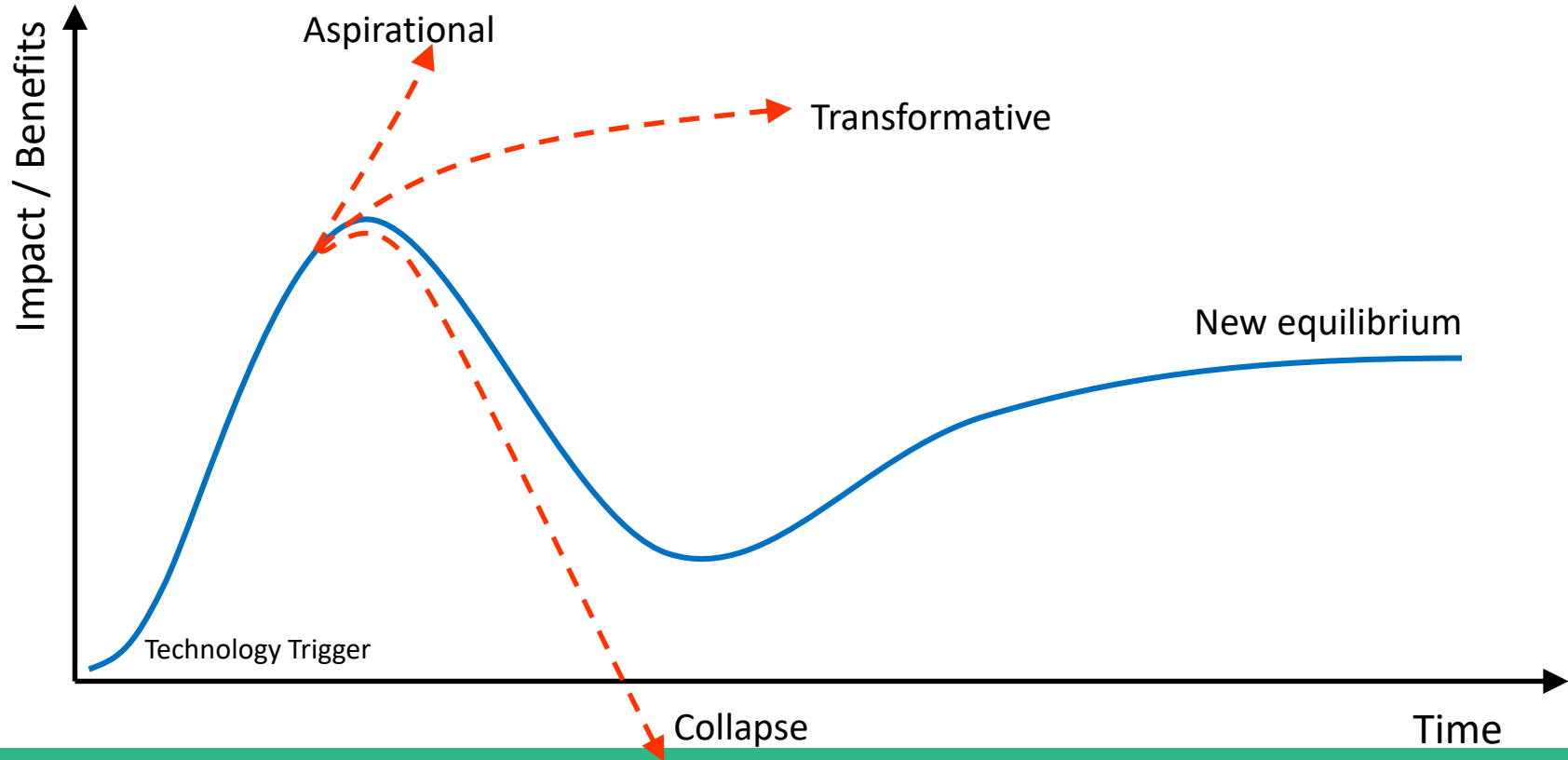
Data61: Blockchain Risks, Opportunities and Future Scenarios

*Distributed Ledgers: Scenarios for the
Australian economy over the coming
decades*

Hanson, R. T., Reeson, A. Staples, M.

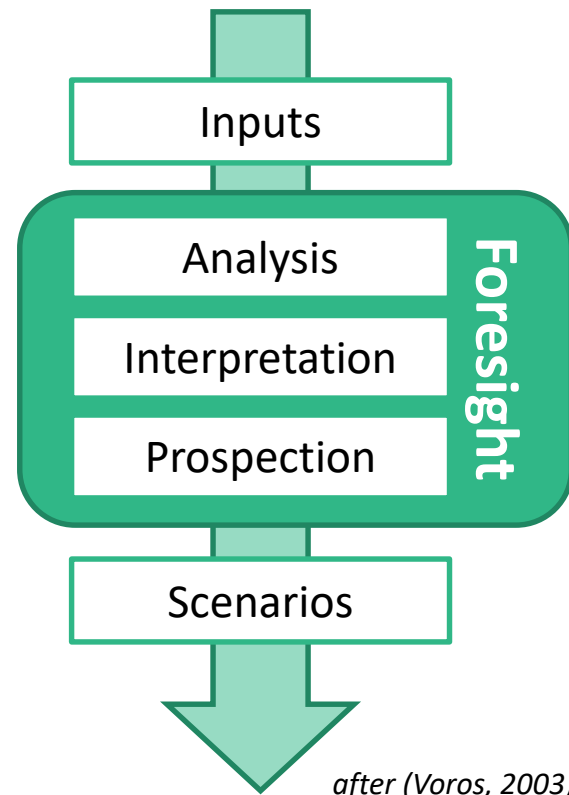
What might plausibly happen, across
society & economy?

Foresight – Plausible Scenarios?



DLT Foresight – Methodology

- Consultative workshops, panel discussion
 - Impact on future of audit (and professional services)
 - Impact on privacy and identity
 - Impact on law, especially contracts
 - Draft scenarios
- Over 100 subject matter experts consulted
 - Government Departments
 - Start-ups
 - Banking and Finance
 - Academics, and
 - Professionals

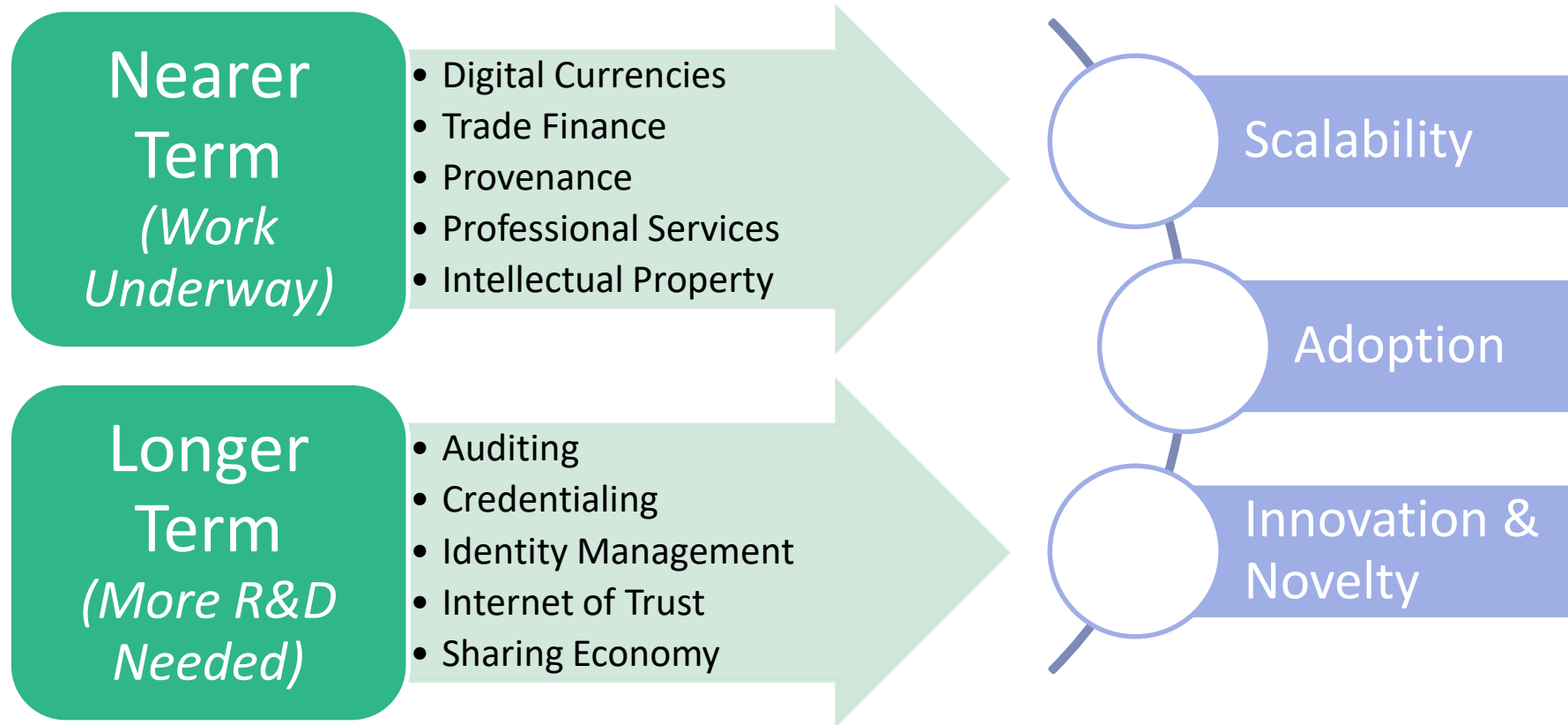


Four Scenarios



1. Regulation on Rails – *Aspirational*
 - Understanding of risk and potential; adoption, innovation, and productivity
 - Leading and cohesive regulatory support and automation
2. Sherriff on the Digital Superhighway – *Transformational*
 - Industry and IoT-led adoption
 - DLT “deputised” for provenance and internet of trust
3. A Bumpy Ride – *New Equilibrium*
 - Proliferation of many DLTs without regulatory acceptance or standards
 - Lack of trust in technology and regulation cripples full DLT potential
4. A Slippery Slope – *Collapse*
 - History of loss, failure, crime, mis-use, “hacks”, and broken trust from DLT
 - Regulatory barriers installed; Abandonment of blockchain as a “brand”

DLT Foresight – Use Cases and Key Issues



DLT Foresight – What's Changed, What's Next?

What's Changed, What's Next?



- Active interest, good & growing understanding by regulators
- Australia leading ISO TC307 standards on Blockchain and DLT
- Still yet to get clear indication of widespread adoption & benefit
- Cryptocurrencies are a two-edged sword for blockchain/DLT
- Massive ongoing technological innovation
 - Interoperability, Governance, Distributed Exchange, Scalability, Privacy



RISKS AND OPPORTUNITIES FOR SYSTEMS USING BLOCKCHAIN AND SMART CONTRACTS

May 2017



Data61: Blockchain Risks, Opportunities and Future Scenarios

Risks and Opportunities for Systems Using Blockchain and Smart Contracts

Staples, M., Chen, S., Falamaki, S.,
Ponomarev, A., Rimba, P., Tran, A. B.,
Weber, I., Xu, X., Zhu, J.

What are technical risks & opportunities
for use cases?

Study Perspectives and Approach

Software Architecture



Non-Functional Properties

- *Security, Performance, ...*



Dependable Software Systems

Trusted and Trustworthy Systems

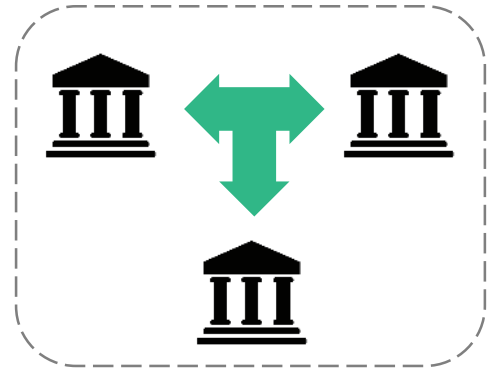
- *Risk, Evidence, Assurance, ...*

- Blockchain are components in broader systems
- Identify plausible use cases
- Create some design alternatives, examine trade-offs
 - Focus on three illustrative contrasting use-cases

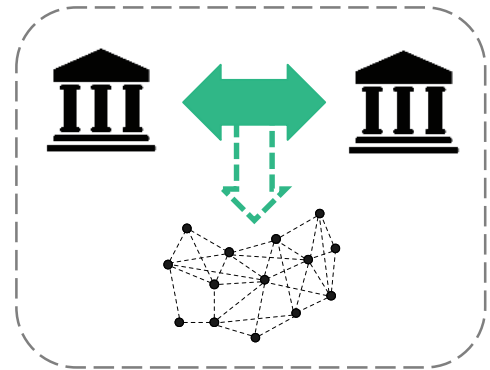
What Does a Blockchain Do?

- Functionally, blockchains are...
- A database (ledger)
 - Record of transactions
- A compute platform
 - “Smart contracts”
- Distributed, and no central owner

**Centralised Trust
using a
Third-Party**



**Distributed Trust
using a
Blockchain**

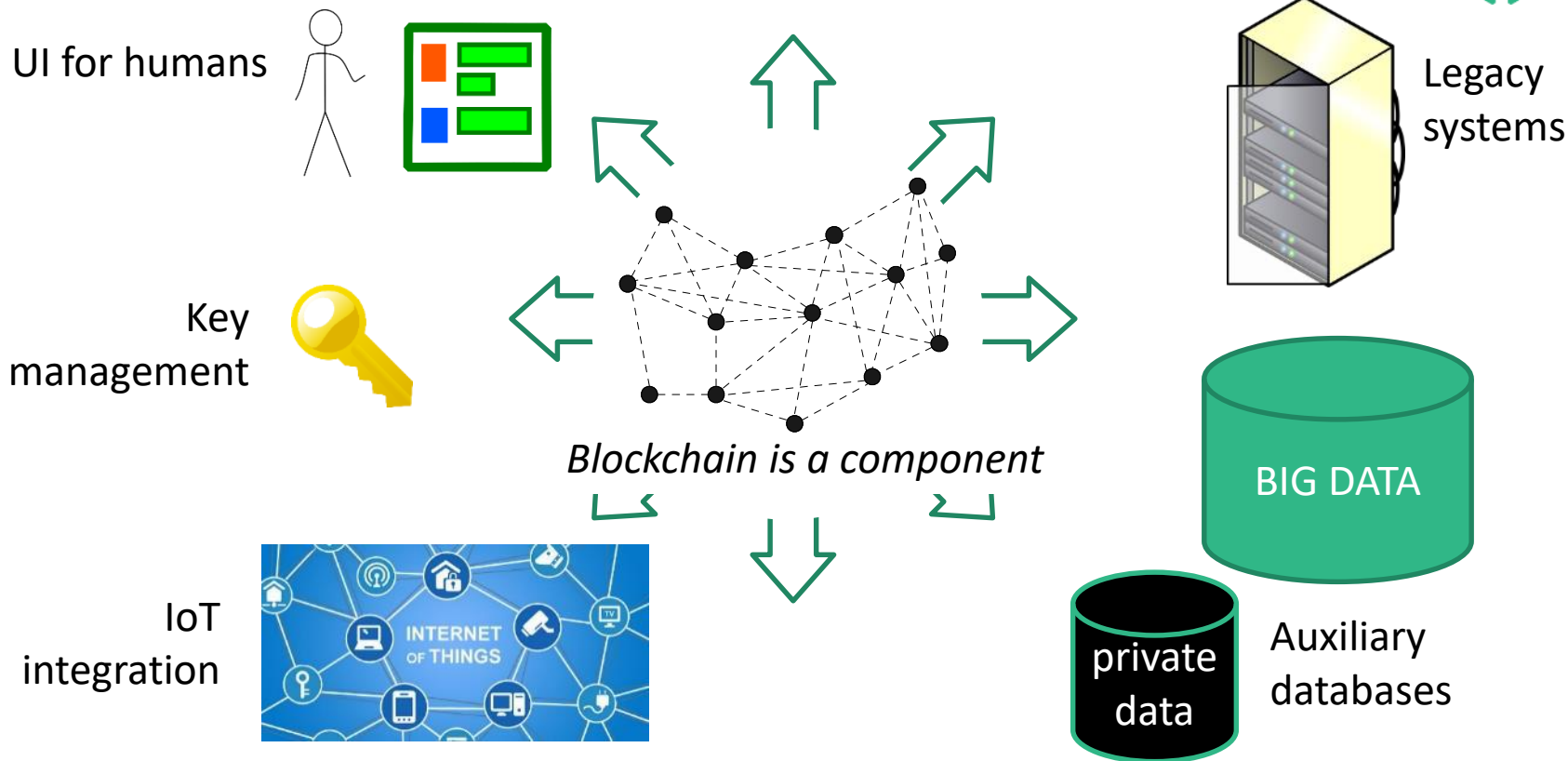


Compared to Conventional Databases



- Logically centralised;
Physically and administratively decentralised
- Trade-offs for Various Non-Functional Properties
 - (+) Integrity, Non-repudiation
 - (-) Confidentiality, Privacy
 - (-) Modifiability
 - (-) Throughput/ Scalability/ Big Data
 - (+ read/ - write) Availability/ Latency

Blockchains are Not Stand-Alone Systems

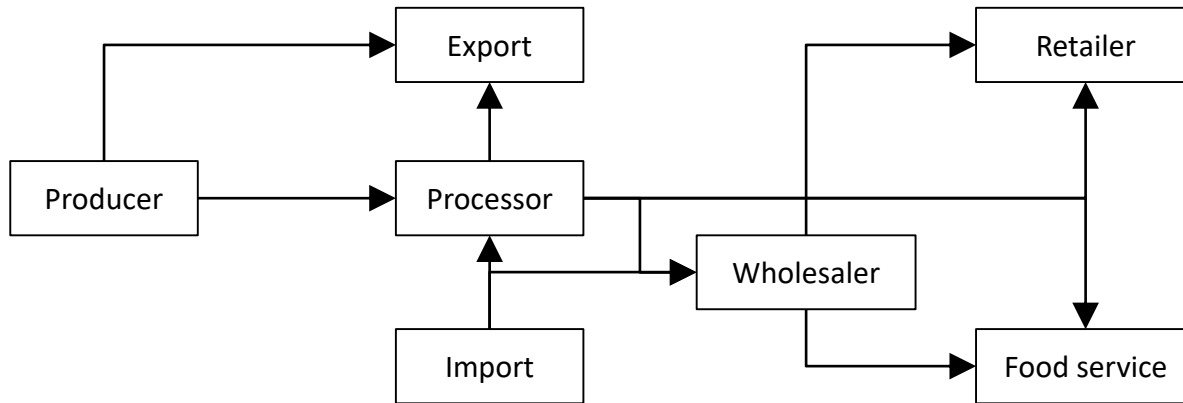


Potential Use Cases



- Financial Services
 - Digital currency
 - (International) payments
 - Reconciliation
 - Settlement
 - Markets
 - Trade finance
- Government Services
 - Registry & Identity
 - Grants & Social Security
 - Quota management
 - Taxation
- Enterprise and Industry
 - Supply chain
 - IoT
 - Metered access
 - Digital rights 7 IP
 - Data management
 - Attestation
 - Inter-divisional accounting
 - Corporate Affairs
- Three Illustrative Cases Selected
 1. Agricultural supply chain
 2. Open data registry
 3. Remittance payments

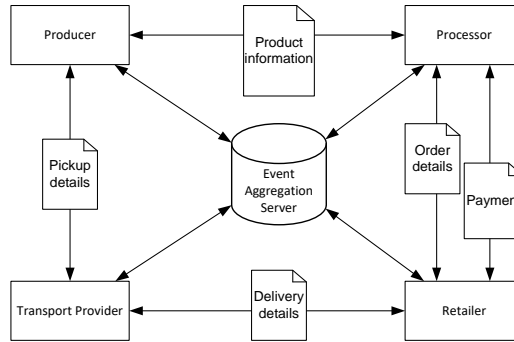
Agricultural Supply Chain – Use Case



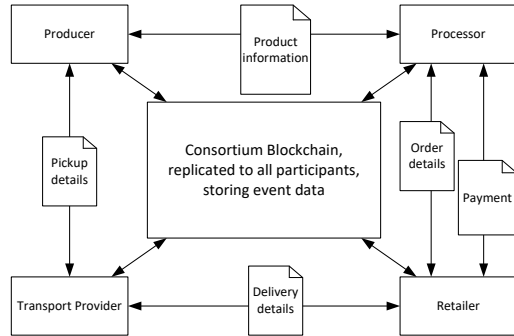
Interoperability
Latency
Integrity
Confidentiality
Scalability

Agricultural Supply Chain – Designs

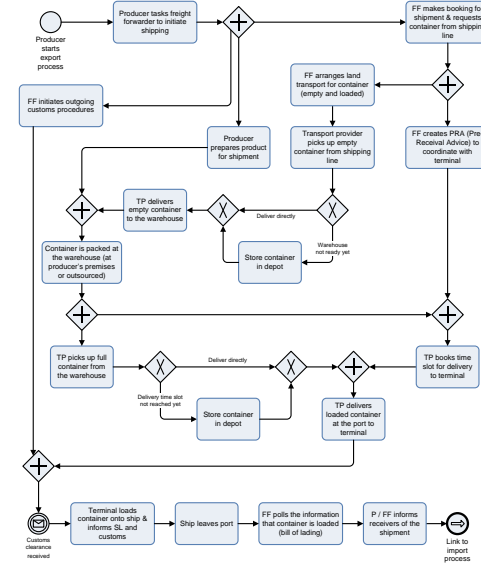
1. Conventional Point-to-point messaging and event aggregation server



2. Event Tracking on Blockchain Point-to-point messaging and event aggregation on blockchain



3. Supply chain process coordination on blockchain as smart contracts

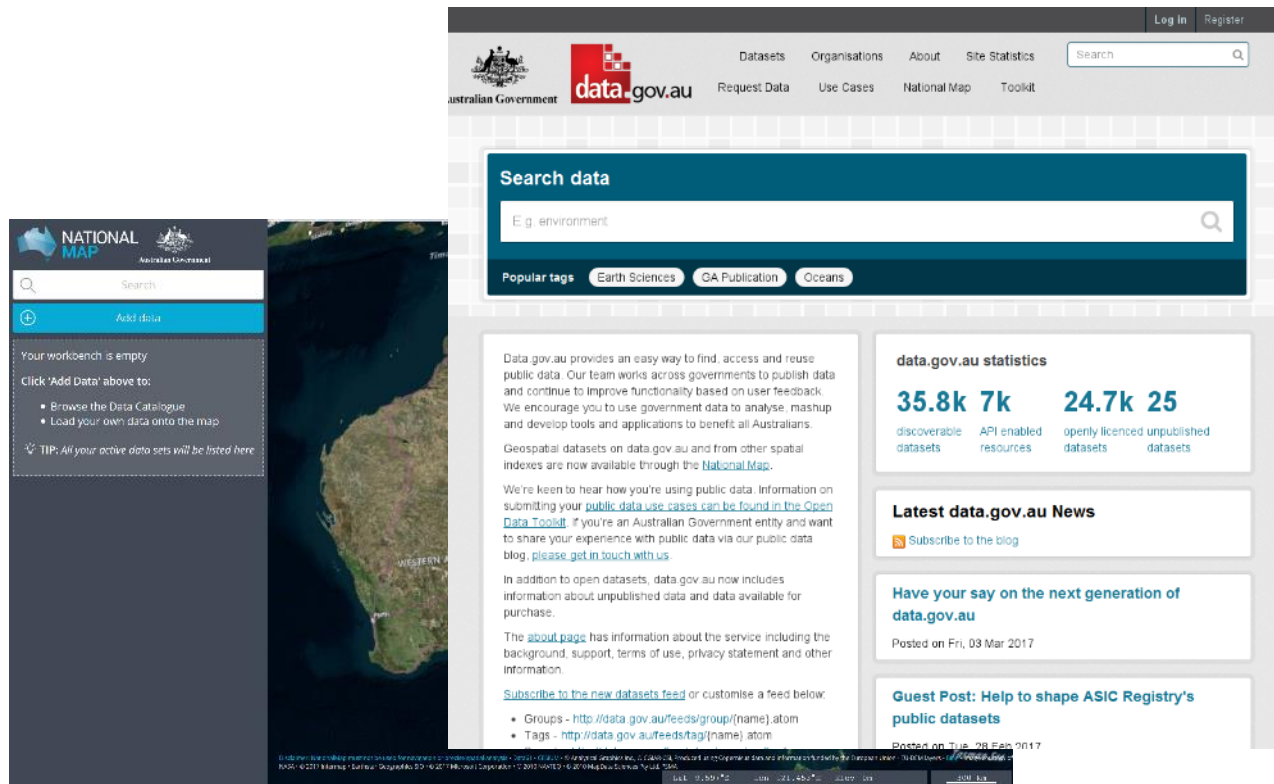


Supply Chain & Trade Finance



- Structure of supply chains similar to blockchain
 - No centre; highly distributed; many parties; dynamic relationships
- Might address limitations in supply chain
 - Limited visibility & logistics efficiency
 - Provenance & Supply chain quality
- But also enables derived financial services
 - Trade Finance
 - Insurance
- Attach financial contracts directly to logistics contracts

Open Data Registries – Use Case

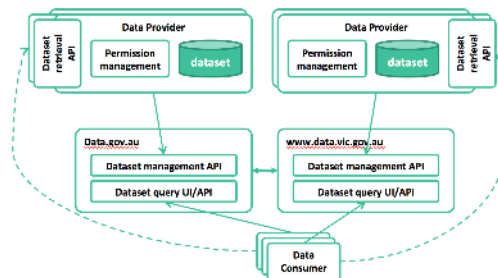


The image shows two overlapping web interfaces. The background interface is the data.gov.au website, which features a search bar with the text "Search data" and "E.g. environment". It also displays "Popular tags" such as "Earth Sciences", "QA Publication", and "Oceans". A statistics section shows "35.8k 7k 24.7k 25" for discoverable, API enabled, openly licenced, and unpublished datasets respectively. The foreground interface is the National Map, showing a map of Australia with a search bar and a sidebar with "Add data" and "Your workbook is empty" options.

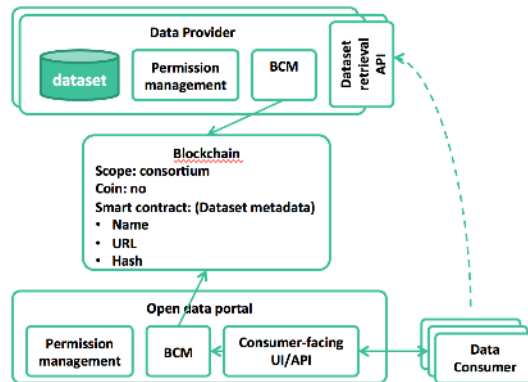
Integrity
Availability
Read Latency
Interoperability
Barriers to access

Open Data Registries – Designs

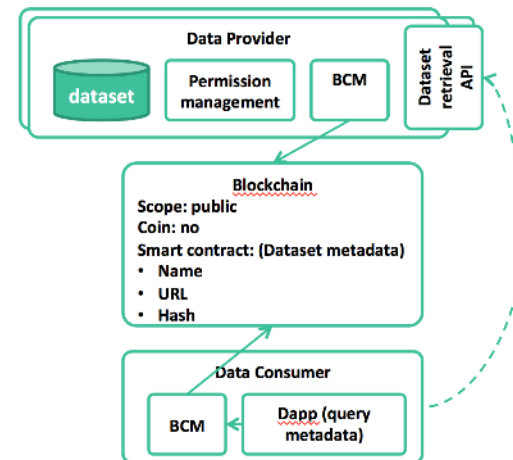
1. Conventional Registry operated by single agency



2. Consortium across data providers Public access still controlled through a portal

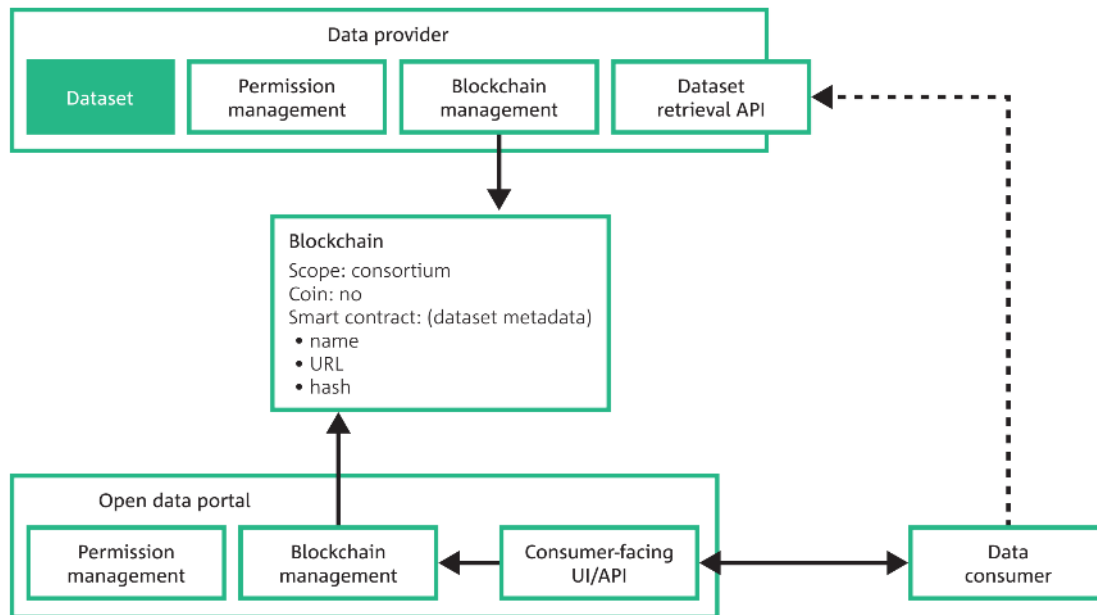


3. Registry on public blockchain Agency only controls entries included on official index



Registries

- Blockchains can help to federate registries
- Sometimes too much integrity causes problems



Open Data Registry

Powered by Ethereum blockchain, Open Data Registry is an open platform for individuals and organisations to share and trade data, as well as performing analytics on data.



6
Datasets



4
Jobs

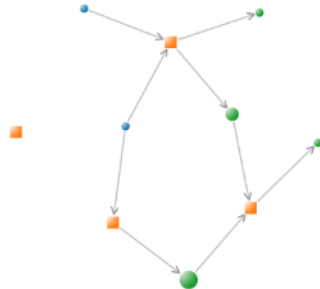


5
Transactions



4.5 ether
Largest Transaction

Data Platform Provenance Graph



Legends

Node Types

- Original Datasets
- Derived Datasets
- Data analytic Jobs

Accumulated Dataset Value

- < 1 szabo
- 1 szabo - 1 ether
- > 1 ether

Search All Datasets

Type keywords to search for datasets...

0X8E61034724E41B4057A2D3101E0E714E7B93F20

Dataset Accumulated Value: 4.5 ether

Owner: X-Analytics

Description: Travel frequency based on travel purpose for people in different cities.

Search



Regerator

Design

Manage

0x1b437e922bf1e4eb430e5345cd5ebf0c9e0939a

Log Out

Create New Registry

DatasetRegistry

Attributes

```
Record
<<PK>> id: uint32
owner: address
title: string
description: string
<<PK>> parent datasets: uint32[]
records: mapping(uint32 => Record)
```

Functions

```
+ record_get_attr_title(record_id)
+ record_get_owner(record_id)
+ record_exists(record_id)
+ record_get_attr_description(record_id)
+ record_get_attr_parent_datasets(record_id)
+ record_get_attr_records(record_id)
+ record_delete(record_id)
+ record_set_attr_parent_datasets(record_id, parent_datasets)
+ record_set_attr_title(record_id, title)
+ record_set_attr_description(record_id, description)
+ record_create(record_id, title, description)
```

Events

```
+ records_history(record_id, owner, creation_timestamp)
+ record_revisions_history(record_id, action_sig, revision_timestamp)
```

FileRegistry

Attributes

```
+ records: address[]
```

Functions

```
+ get_all_record_ids()
+ admin_get_attr_external_refs()
+ record_exists(record_id)
+ record_set_attr_dataset_id(record_id, dataset_id)
+ record_create(name, url)
+ record_set_attr_name(record_id, name)
+ record_set_attr_url(record_id, url)
+ record_delete(record_id)
+ admin_set_attr_referenced_registry_Dataset(Dataset_registry)
```

Events

```
+ records_history(record_id, owner, creation_timestamp)
```

FileRecord

Attributes

```
<<PK>> id: address
owner: address
name: string
url: string
<<PK>> dataset_id: uint32
```

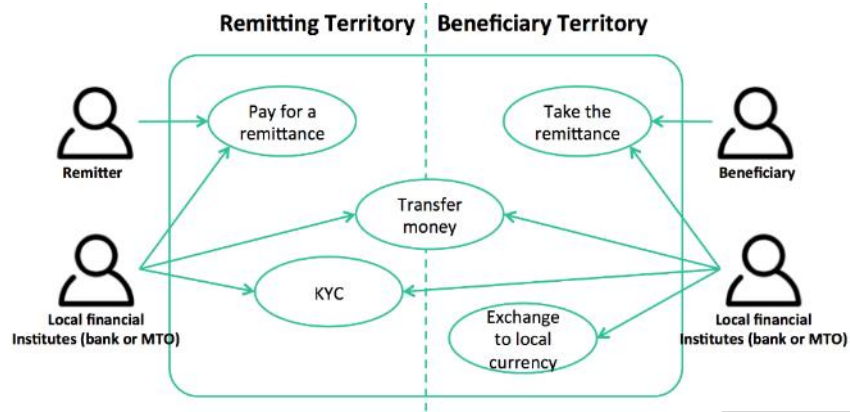
Functions

```
+ record_get_state()
+ record_get_attr_dataset_id()
+ managing_registry()
+ record_get_attr_name()
+ record_exists()
+ record_get_owner()
+ record_get_attr_url()
+ record_set_attr_url(dataset_id)
+ record_set_attr_name(name)
+ record_delete()
```

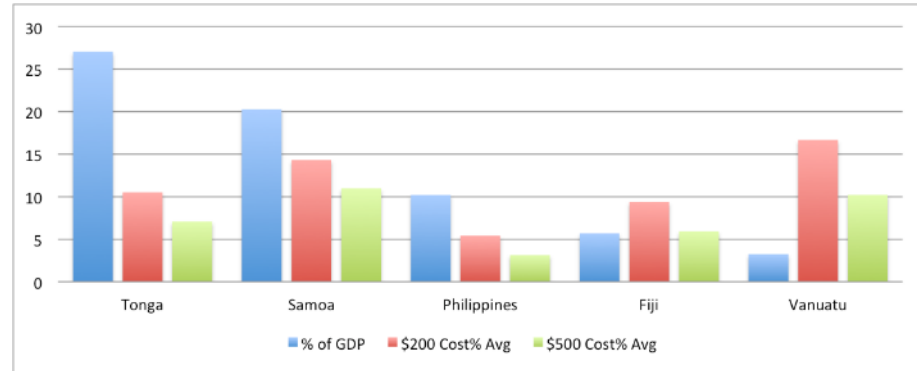
Events

```
+ record_revisions_history(action_sig, revision_timestamp)
```


Remittance Payments – Use Case

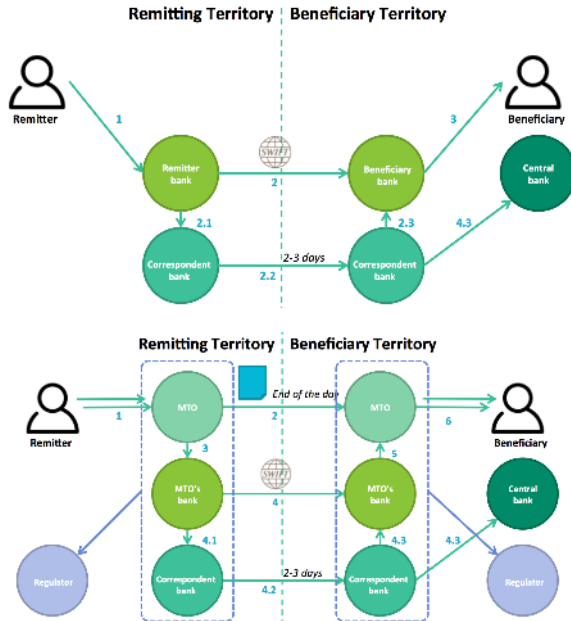


Write Latency
Cost
Cost transparency
Controlled confidentiality
Low barriers to entry

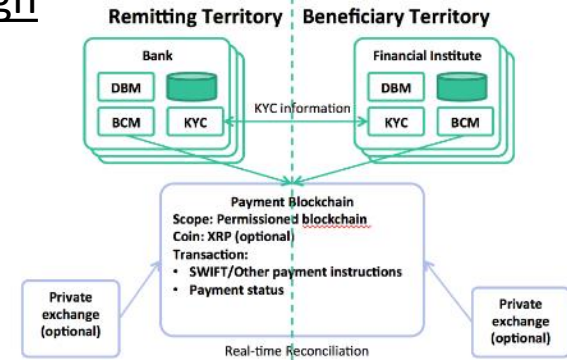


Remittance Payments – Designs

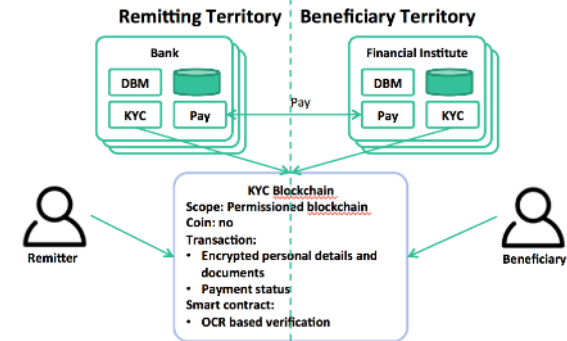
1. Conventional Through bank or MTO



2. Payment through blockchain

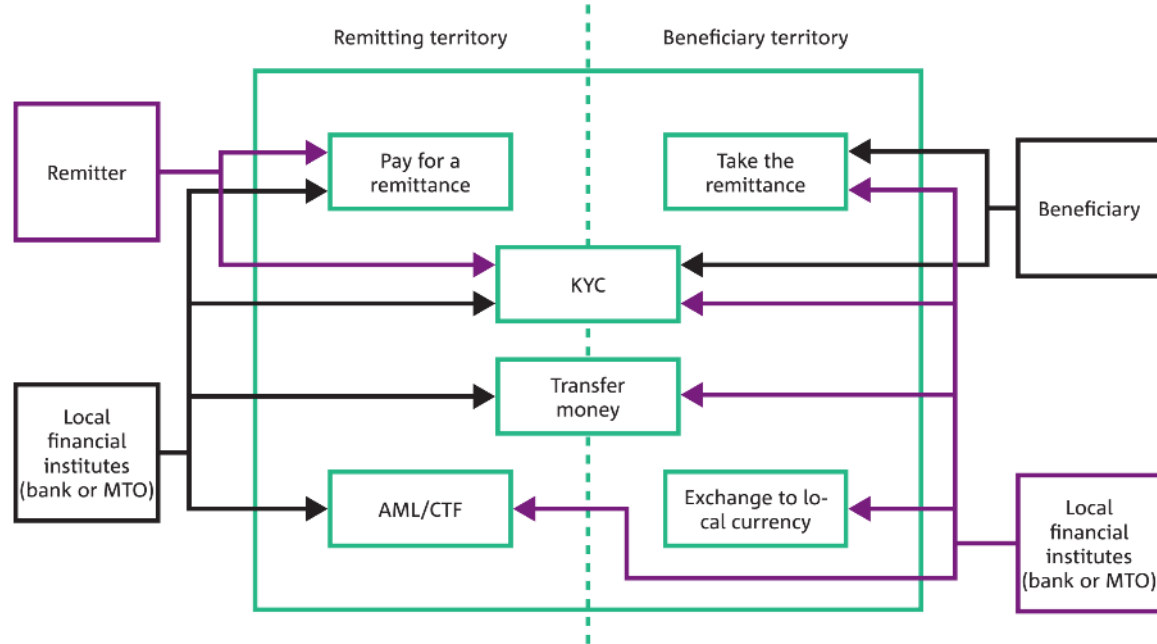


3. KYC through blockchain



Remittances

- Blockchains may help reduce cost and time of remittances, but challenges remain for solutions to KYC
- Blockchains and smart contracts may make it possible to create 'programmable money'



We (Will) Rely on Blockchain-Based Systems



- DAO failure; Parity bug; Phish; Hacking
 - Costs \$60M? \$280M? \$225M in 2017? \$500M + ...?



- Huge future economic value (the main point!)
 - e.g. supply chain, asset registries, settlement, ...



- Security-critical and Safety-critical use cases
 - e.g. e-health records, pharma supply chain, IoT management, ...

What is “Trust”?

Dependable Software Systems says...

- Trusted System

- A system you have chosen to rely on to fulfil a goal
 - When it fails, you suffer harm or loss

- Trustworthy System

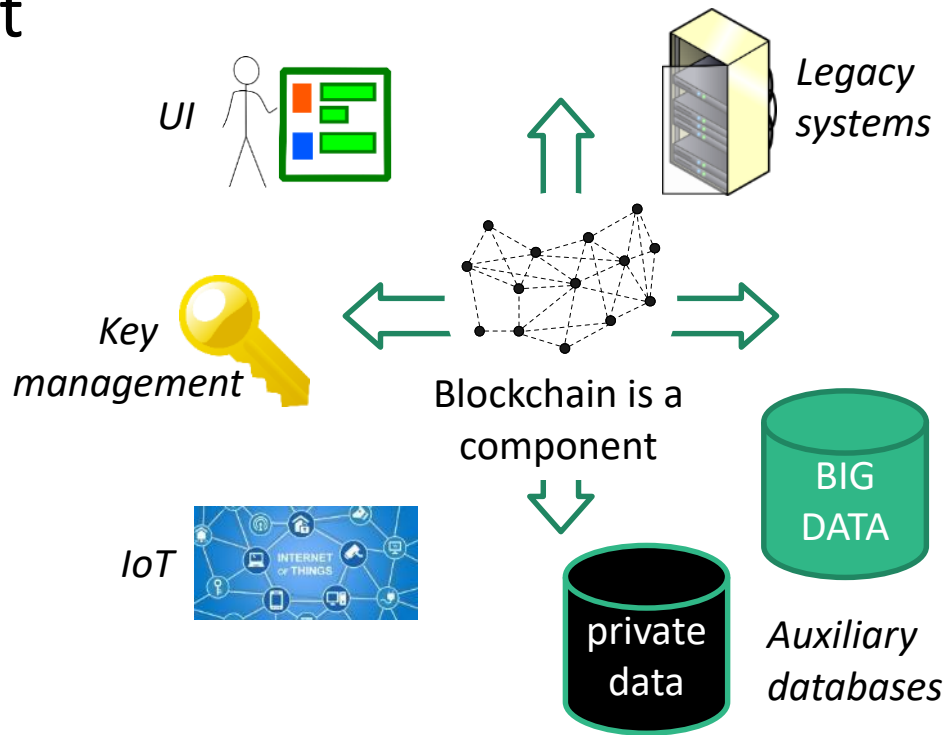
- A system where you have evidence it will not fail



“Trust”
means
accepting
exposure
to risk

Trustworthy Blockchain-Based Systems?

- What is good evidence that blockchain-based systems will do what we need?
 - Functional correctness
 - Non-Functional properties
- How do we get regulatory acceptance?



Assurance: Evidence & Acceptance



- Test blockchains in the rain
- Technologically-neutral regulation and policy
- But look carefully at blockchain-specific risks
- Need indicative guidance on regulatory acceptance of blockchain-based systems
- There are open questions about blockchain governance
- Increase R&D on trustworthy blockchains!

Other Findings



- Blockchains have a different cost model
- Private blockchains are often not private enough
- Public blockchains might be OK for some purposes, even in regulated industries
- Blockchains have limitations – sometimes that doesn't matter!

Busting Blockchain Myths

| Myth | Reality |
|-------------------------------------|--|
| Solves Every Problem | A kind of database |
| Trustless | Can shift trust and spread trust |
| Secure | Focus is Integrity, not Confidentiality |
| Smart contracts are legal contracts | May help execute parts of some legal contracts |
| Immutable | Many only offer probabilistic immutability |
| Need to waste electricity | Emerging blockchains are more efficient |
| Are inherently unscalable | Emerging blockchains are more scalable |
| If beneficial, will be adopted | Adoption can be hampered by FUD |

Risks & Opportunities – What's Changed, What's Next?

What's Changed, What's Next?



- “Programmable money”?
 - What distinctive value for blockchain after NPP + Open Banking?
 - RBA Governor speech indicates possible business cases, especially for B2B
- Data61 blockchain research continues
 - Business process, architecture, availability, consensus, IoT, ...
 - Programmable money
 - Smart contract formal verification (Isabelle) & specification (deontic defeasible)
 - *Towards verifying Ethereum smart contract bytecode in Isabelle/HOL, CPP 2018.*
 - *Evaluation of Logic-Based Smart Contracts for Blockchain Systems, RuleML 2016.*
- Blockchain/DLT is a strategically important avenue in Data61 & CSIRO for supply chain, provenance, and industry integrity infrastructure

Closing Thoughts

Closing Thoughts



- Like the web in mid-90s
 - Industry is in early stages of discovering applications
 - Technology is still rapidly changing
- We are still learning...
 - What the requirements are
 - How to design blockchain-based systems
 - How to provide evidence they are trustworthy
- Some large failures and mis-use have occurred
- Regulation and standards are emerging
- Need more research & more translation of research to industry



Thanks!

Questions?

www.csiro.au

