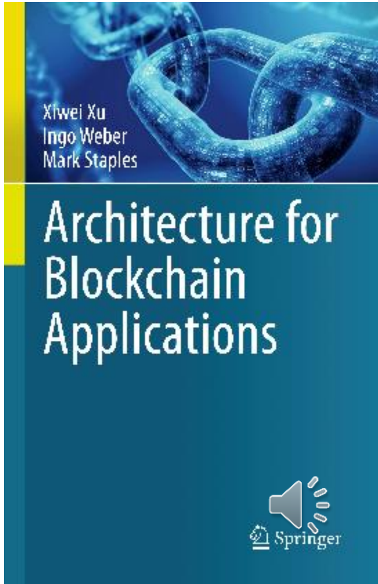
# COMP6452 Guest Lecture

## Some Data61 Blockchain Projects

Dr Mark Staples | 5 August 2020

# Dr Mark Staples

- Blockchain Technologist
  - Co-author of public reports for Australian Treasury in 2017
  - Australia/ISO Blockchain and DLT Standards Committee
  - OECD’s Blockchain Expert Policy Advisory Board
  - Australia’s National Blockchain Roadmap Steering Committee
- Previous Industrial Software & Systems Engineering
  - SCADA; Electronic Payments; Active Implanted Medical Device
  - Director for v1 of Data Standards for Consumer Data Right
- Engineering/Technology Researcher
  - Software Architecture, Formal Methods, Product Lines, Epistemology
  - PhD @U Cambridge (Computer Science)
  - Undergrad @U Queensland (Computer & Cognitive Science)



Xiwei Xu
Ingo Weber
Mark Staples

Architecture for Blockchain Applications

Springer

# Today: Some Data61 Projects

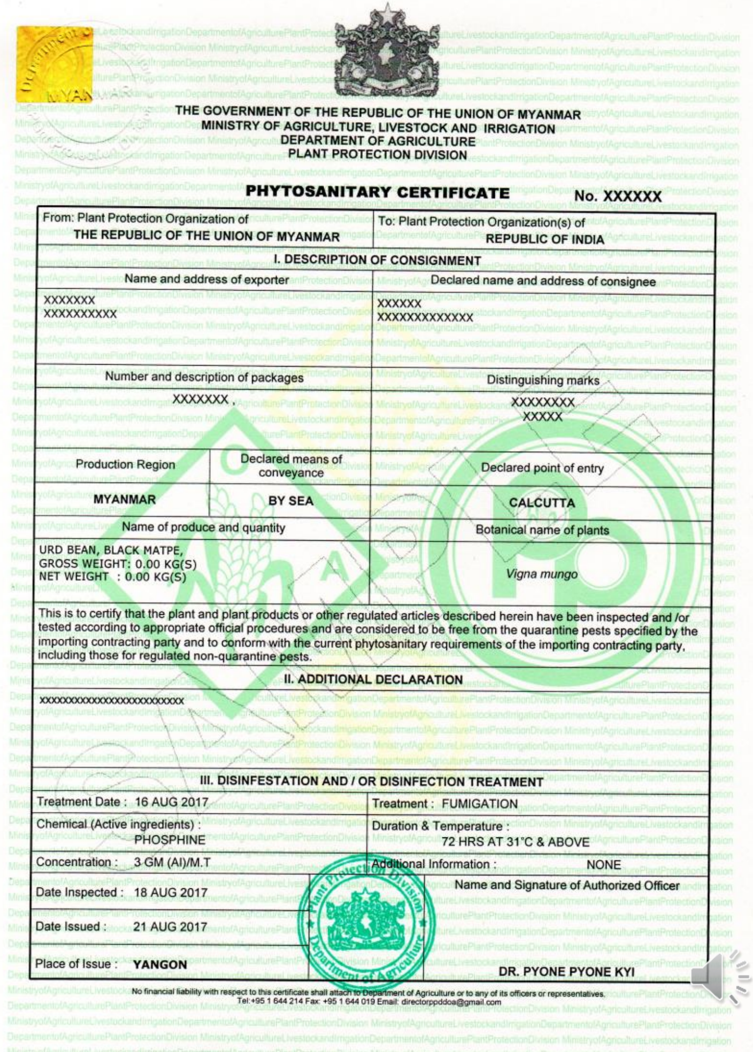
- Often commercial-in-confidence with industry, but these are lab-based proof-of-concept projects
  - ePhyto
    - (combine central global DB with global blockchain overlay)
  - Single Window
    - (blockchain to link siloed databases in large enterprise, behind a web API)
  - Making Money Smart
    - (put policies in tokens; integrate offchain functions like payment)

- Some Concluding Thoughts

# “Augmenting ePhyto”

# ePhyto Certificate

- Electronic equivalent of data paper phytosanitary certificates
- Sent from the national plant protection organisation (NPPO) of the exporting country to the NPPO of the importing country
- Produced, transmitted and received in XML
- Easily converted to e.g. PDF



THE GOVERNMENT OF THE REPUBLIC OF THE UNION OF MYANMAR
MINISTRY OF AGRICULTURE, LIVESTOCK AND IRRIGATION
DEPARTMENT OF AGRICULTURE
PLANT PROTECTION DIVISION

**PHYTOSANITARY CERTIFICATE** No. XXXXXX

| | |
|---|---|
| From: Plant Protection Organization of<br>THE REPUBLIC OF THE UNION OF MYANMAR | To: Plant Protection Organization(s) of<br>REPUBLIC OF INDIA |

I. DESCRIPTION OF CONSIGNMENT

| | | |
|---|---|---|
| Name and address of exporter | | Declared name and address of consignee |
| XXXXXXX<br>XXXXXXXXXX | | XXXXXX<br>XXXXXXXXXXXXX |
| Number and description of packages | | Distinguishing marks |
| XXXXXXX , | | XXXXXXXX<br>XXXXX |
| Production Region | Declared means of conveyance | Declared point of entry |
| MYANMAR | BY SEA | CALCUTTA |
| Name of produce and quantity | | Botanical name of plants |
| URD BEAN, BLACK MATPE,<br>GROSS WEIGHT: 0.00 KG(S)<br>NET WEIGHT : 0.00 KG(S) | | *Vigna mungo* |

This is to certify that the plant and plant products or other regulated articles described herein have been inspected and /or tested according to appropriate official procedures and are considered to be free from the quarantine pests specified by the importing contracting party and to conform with the current phytosanitary requirements of the importing contracting party, including those for regulated non-quarantine pests.

II. ADDITIONAL DECLARATION

xxxxxxxxxxxxxxxxxxxxxxxxx

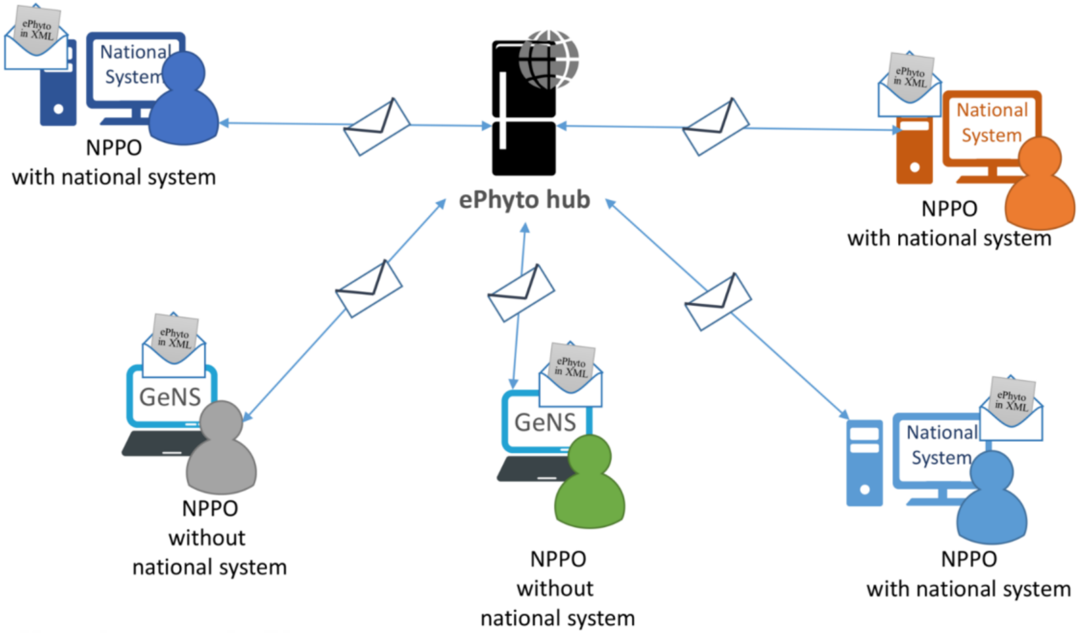
III. DISINFESTATION AND / OR DISINFECTION TREATMENT

| | |
|---|---|
| Treatment Date : 16 AUG 2017 | Treatment : FUMIGATION |
| Chemical (Active ingredients) :<br>PHOSPHINE | Duration & Temperature :<br>72 HRS AT 31°C & ABOVE |
| Concentration : 3 GM (AI)/M.T | Additional Information : NONE |
| Date Inspected : 18 AUG 2017 | Name and Signature of Authorized Officer |
| Date Issued : 21 AUG 2017 | |
| Place of Issue : YANGON | DR. PYONE PYONE KYI |

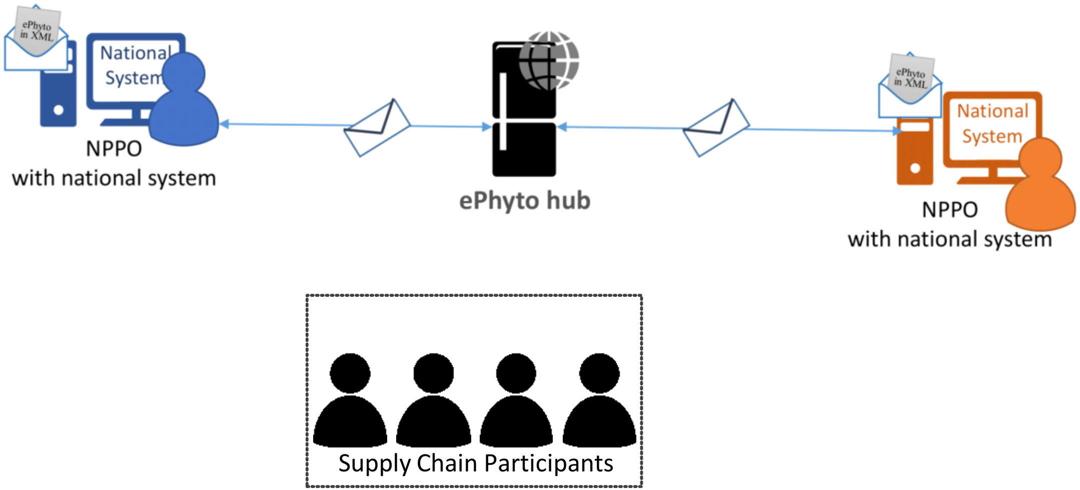
Plant Protection Division · Department of Agriculture

No financial liability with respect to this certificate shall attach to Department of Agriculture or to any of its officers or representatives.
Tel:+95 1 644 214 Fax: +95 1 644 019 Email: directorppddoa@gmail.com

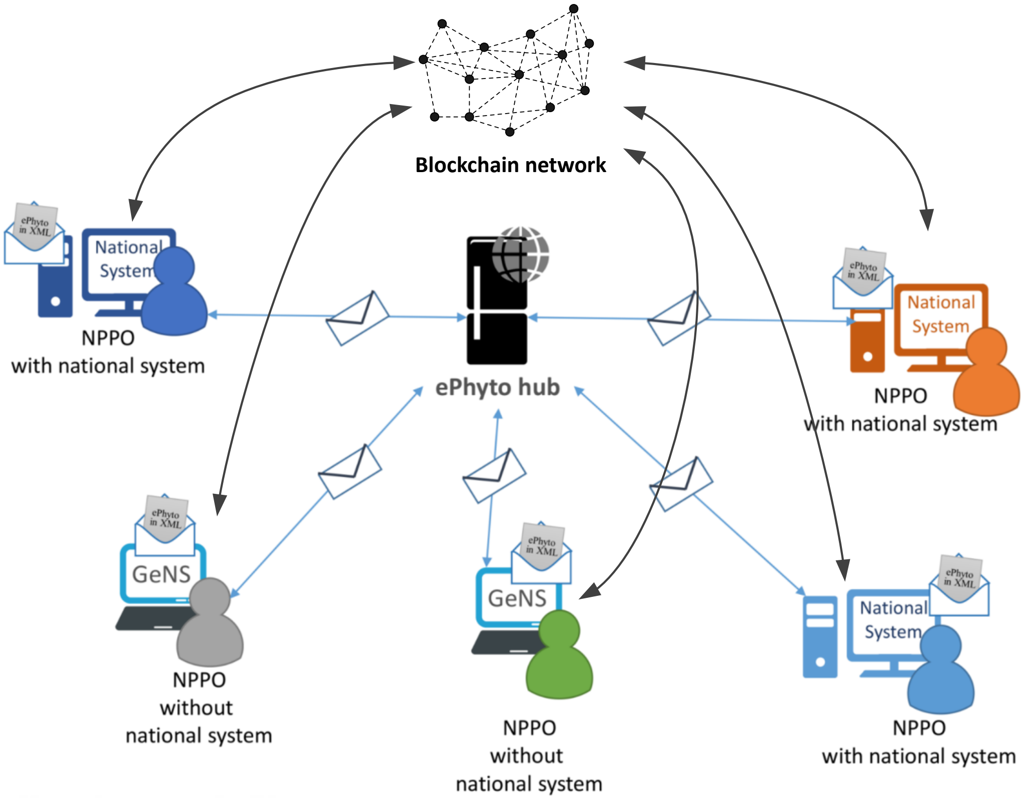
# IPPC system


ePhyto in XML
National System
NPPO
with national system
ePhyto hub
ePhyto in XML
National System
NPPO
with national system
ePhyto in XML
GeNS
NPPO
without
national system
ePhyto in XML
GeNS
NPPO
without
national system
ePhyto in XML
National System
NPPO
with national system

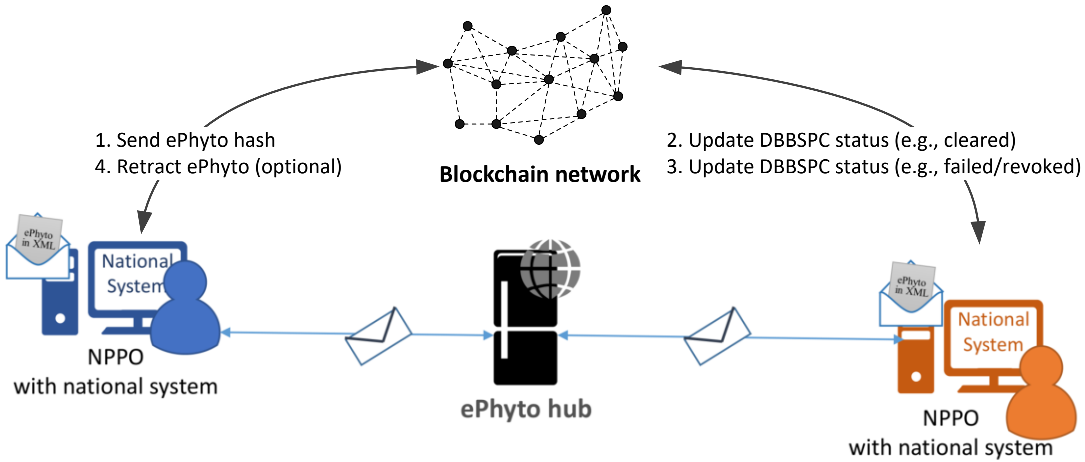
# What About Other Parties?



# Proposed amendment

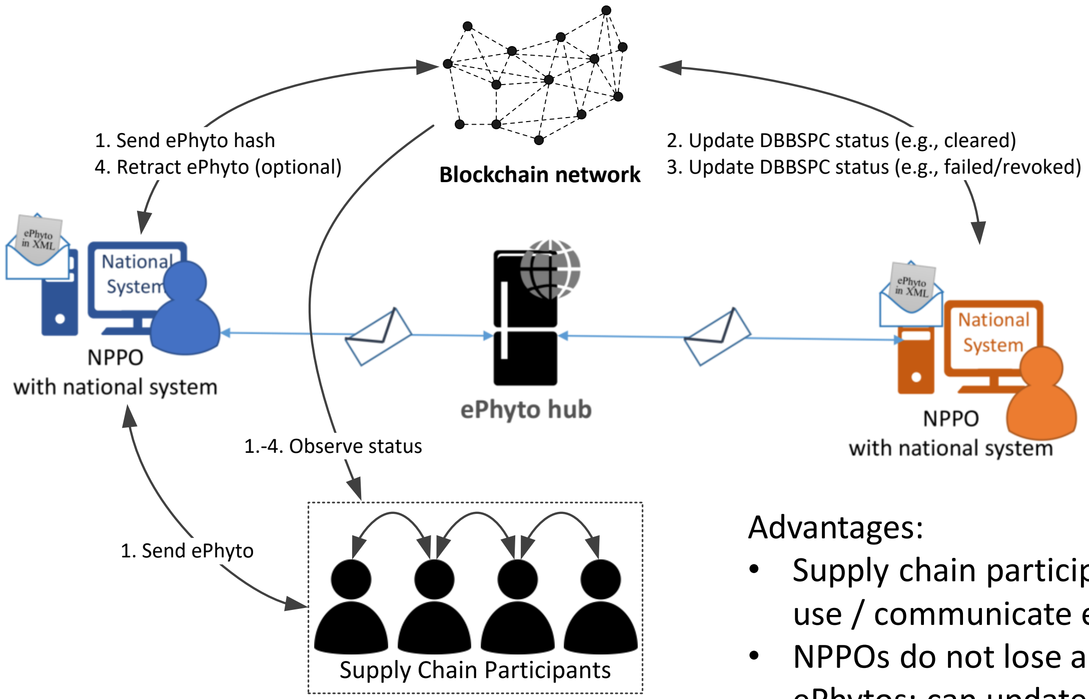


# Proposed amendment – Detail 1



*DBBSPC: Document-Based BioSecurity PreClearance

# Proposed amendment – Detail 2



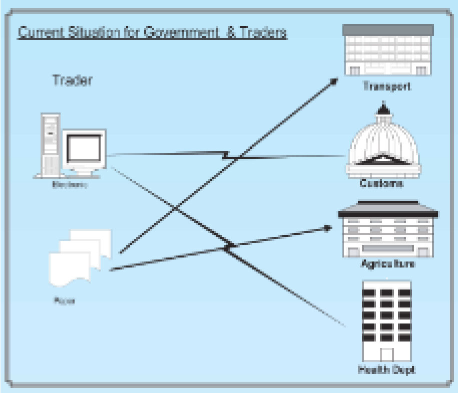
Advantages:

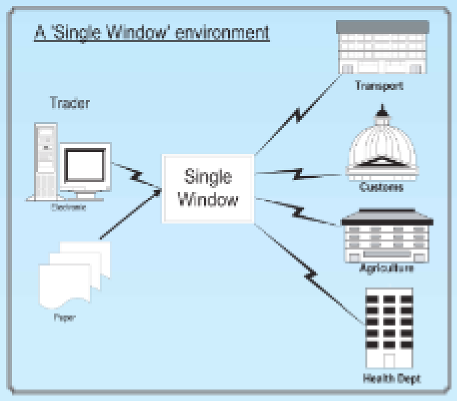
- Supply chain participants can access / use / communicate ePhytos
- NPPOs do not lose authority over ePhytos: can update/retract them
- Minimal change to IPPC system

*DBBSPC: Document-Based BioSecurity PreClearance

# “Blockchain Single Window”

# Single Window on Blockchain?

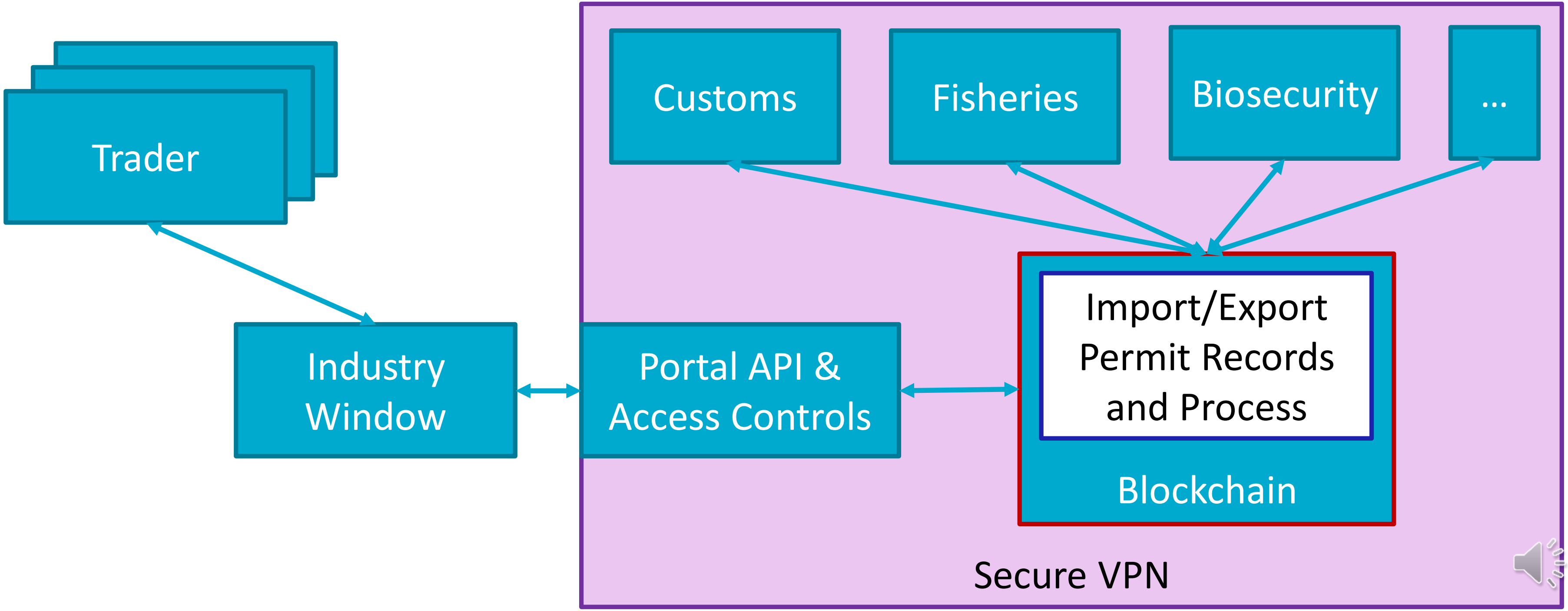


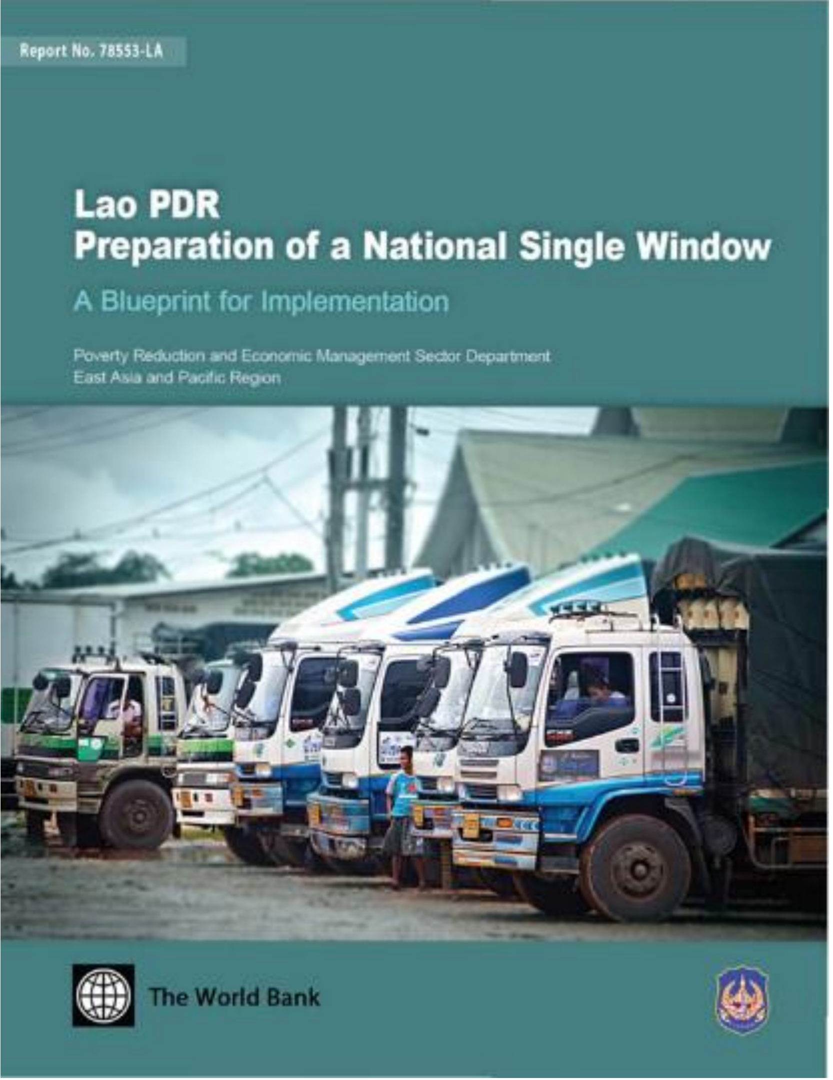


(UNECE) *The Single Window Concept: enhancing the efficient exchange of information between trade and government*

- Lab-based exploration using real-world process model
  - Logically centralised; administratively decentralised
  - Single source of truth on import/export approvals
  - Smart contracts for flexible process
  - Auditability

# Lab Study of Blockchain Single Window





Report No. 78553-LA

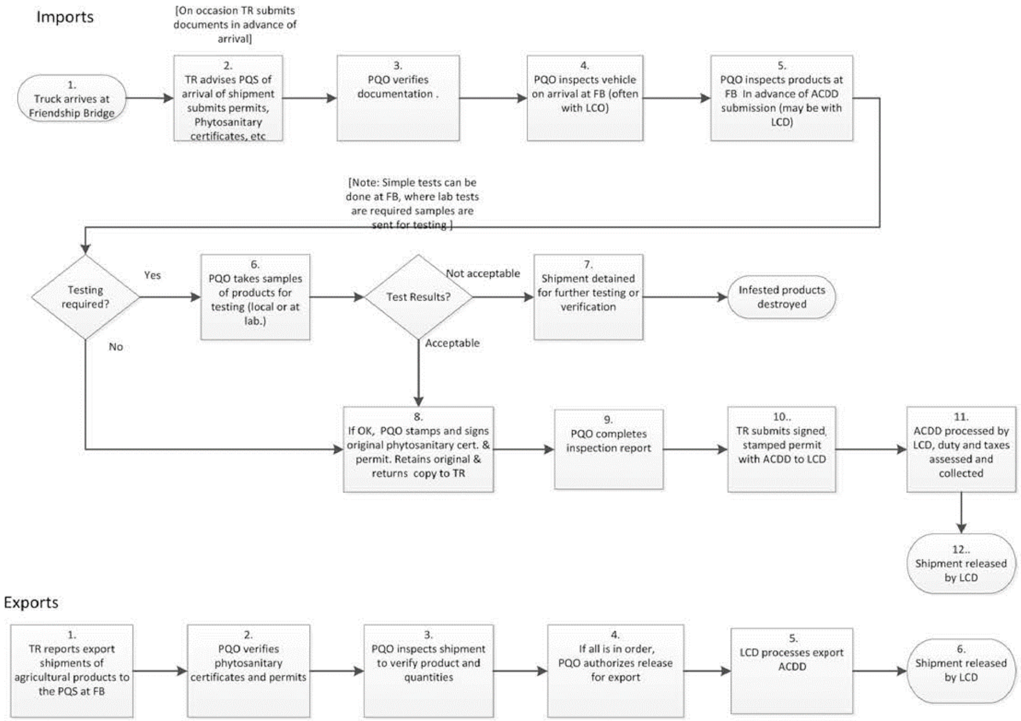
# Lao PDR
# Preparation of a National Single Window

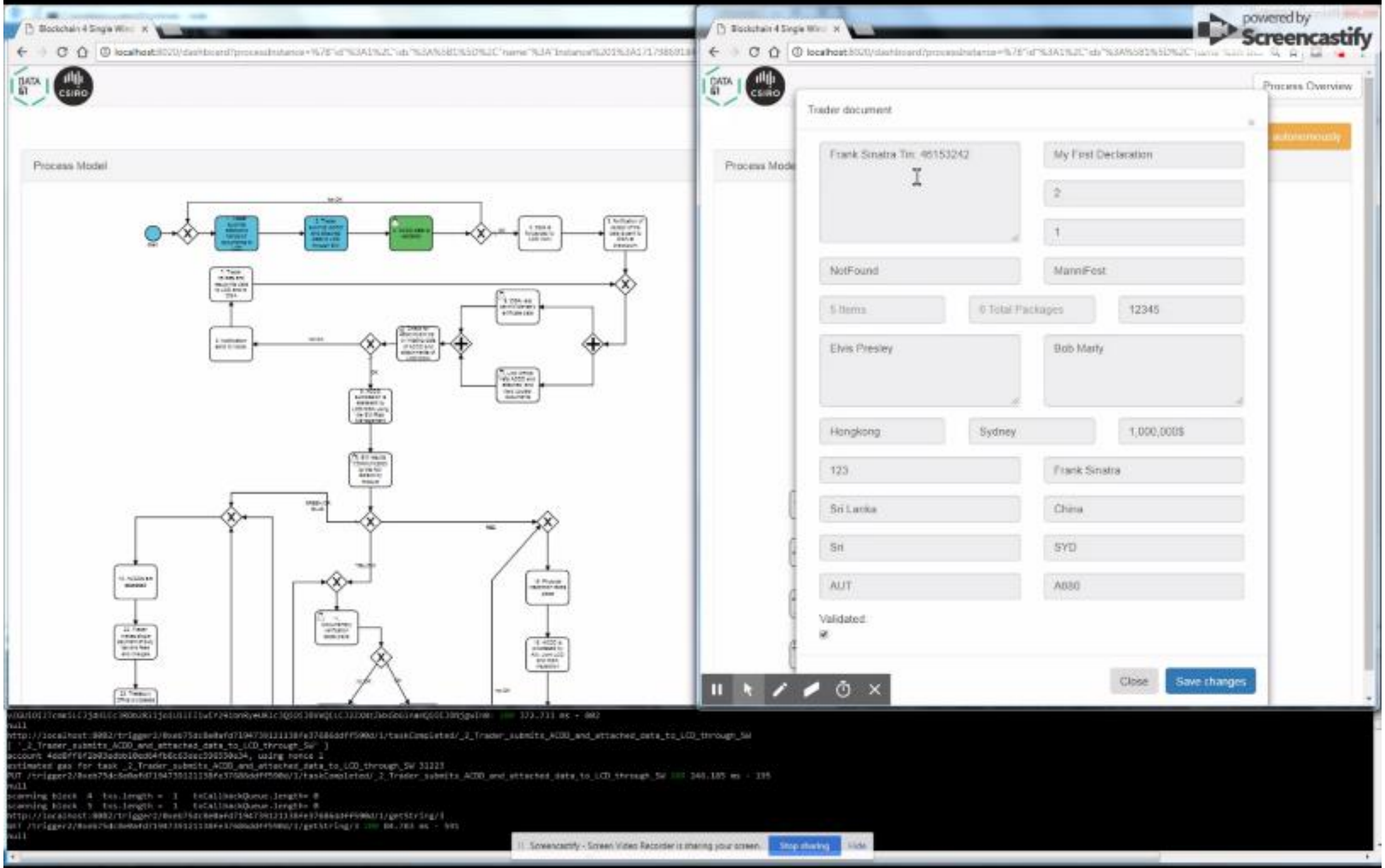
## A Blueprint for Implementation

Poverty Reduction and Economic Management Sector Department
East Asia and Pacific Region

The World Bank

PQ – 01 Procedures for processing imports/exports of Agricultural Products at Friendship Bridge/Thanaleng Border Crossing


Imports
[On occasion TR submits documents in advance of arrival]
1. Truck arrives at Friendship Bridge
2. TR advises PQS of arrival of shipment submits permits, Phytosanitary certificates, etc
3. PQO verifies documentation .
4. PQO inspects vehicle on arrival at FB (often with LCO)
5. PQO inspects products at FB In advance of ACDD submission (may be with LCD)
[Note: Simple tests can be done at FB, where lab tests are required samples are sent for testing ]
Testing required?
Yes
No
6. PQO takes samples of products for testing (local or at lab.)
Test Results?
Not acceptable
Acceptable
7. Shipment detained for further testing or verification
Infested products destroyed
8. If OK, PQO stamps and signs original phytosanitary cert. & permit. Retains original & returns copy to TR
9. PQO completes inspection report
10.. TR submits signed, stamped permit with ACDD to LCD
11. ACDD processed by LCD, duty and taxes assessed and collected
12.. Shipment released by LCD
Exports
1. TR reports export shipments of agricultural products to the PQS at FB
2. PQO verifies phytosanitary certificates and permits
3. PQO inspects shipment to verify product and quantities
4. If all is in order, PQO authorizes release for export
5. LCD processes export ACDD
6. Shipment released by LCD



Trader document

| | | |
|---|---|---|
| Frank Sinatra Tin: 46153242 | My First Declaration | |
| | 2 | |
| | 1 | |
| NotFound | ManniFest | |
| 5 Items | 0 Total Packages | 12345 |
| Elvis Presley | Bob Marly | |
| Hongkong | Sydney | 1,000,000$ |
| 123 | Frank Sinatra | |
| Sri Lanka | China | |
| Sri | SYD | |
| AUT | A880 | |

Validated:
☑

Close
Save changes

```
[illegible] 200 372.733 ms - 882
null
http://localhost:8082/trigger2/[illegible]/1/taskCompleted/_2_Trader_submits_ACDD_and_attached_data_to_LCD_through_SW
[ '_2_Trader_submits_ACDD_and_attached_data_to_LCD_through_SW' ]
account 4dd[illegible], using nonce 1
estimated gas for task _2_Trader_submits_ACDD_and_attached_data_to_LCD_through_SW 31223
PUT /trigger2/[illegible]/1/taskCompleted/_2_Trader_submits_ACDD_and_attached_data_to_LCD_through_SW 200 240.185 ms - 335
null
scanning block  4  txs.length =  1   toCallbackQueue.length= 0
scanning block  5  txs.length =  1   toCallbackQueue.length= 0
http://localhost:8082/trigger2/[illegible]/1/getString/1
GET /trigger2/[illegible]/1/getString/1 200 84.783 ms - 595
null
```

Screencastify - Screen Video Recorder is sharing your screen.
Stop sharing
Hide

# “Making Money Smart”

# Making Money Smart

https://data61.csiro.au/en/Our-Work/SmartMoney

http://www.commbank.com.au/makingmoneysmart

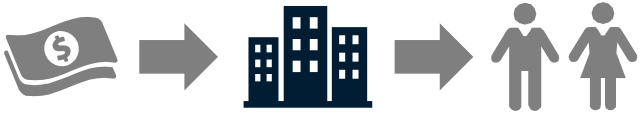
CommonwealthBank of Australia

CSIRO DATA 61

# The NDIS provides greater choice and control for participants

**PREVIOUSLY**

Block funding to providers

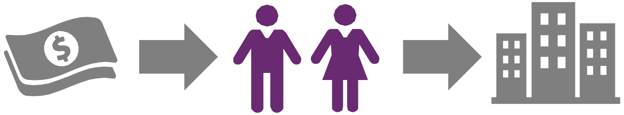


**Limited incentives** to reduce costs, improve quality and innovate

TO

ndis

Direct funding to participants



Providing people with disability with greater **choice and control**

# But with greater choice and control, comes challenges

### Challenge 1

Plan budget information is not always available

### Challenge 2

Service eligibility is not always straightforward

### Challenge 3

Payments and reconciliation can be complex for providers

### Challenge 4

Manual audits are required to manage misspending risks

### Challenge 5

Unlocked potential to leverage plan data

CSIRO DATA 61

# We engaged a broad range of stakeholders

**7** Participants

and

**3** Carers

for formal user testing

**19** Senior Managers

and Staff from

**4** Service

Providers

newhorizons
wellbeing. done well.

**10** Disability sector

experts from

**5** Organisations

**29**

Leaders and/or Staff from the Reference Group of

**12** Government Agencies and Industry Bodies

**8** Volunteers

from the Commonwealth Bank Friends of the Lab Network

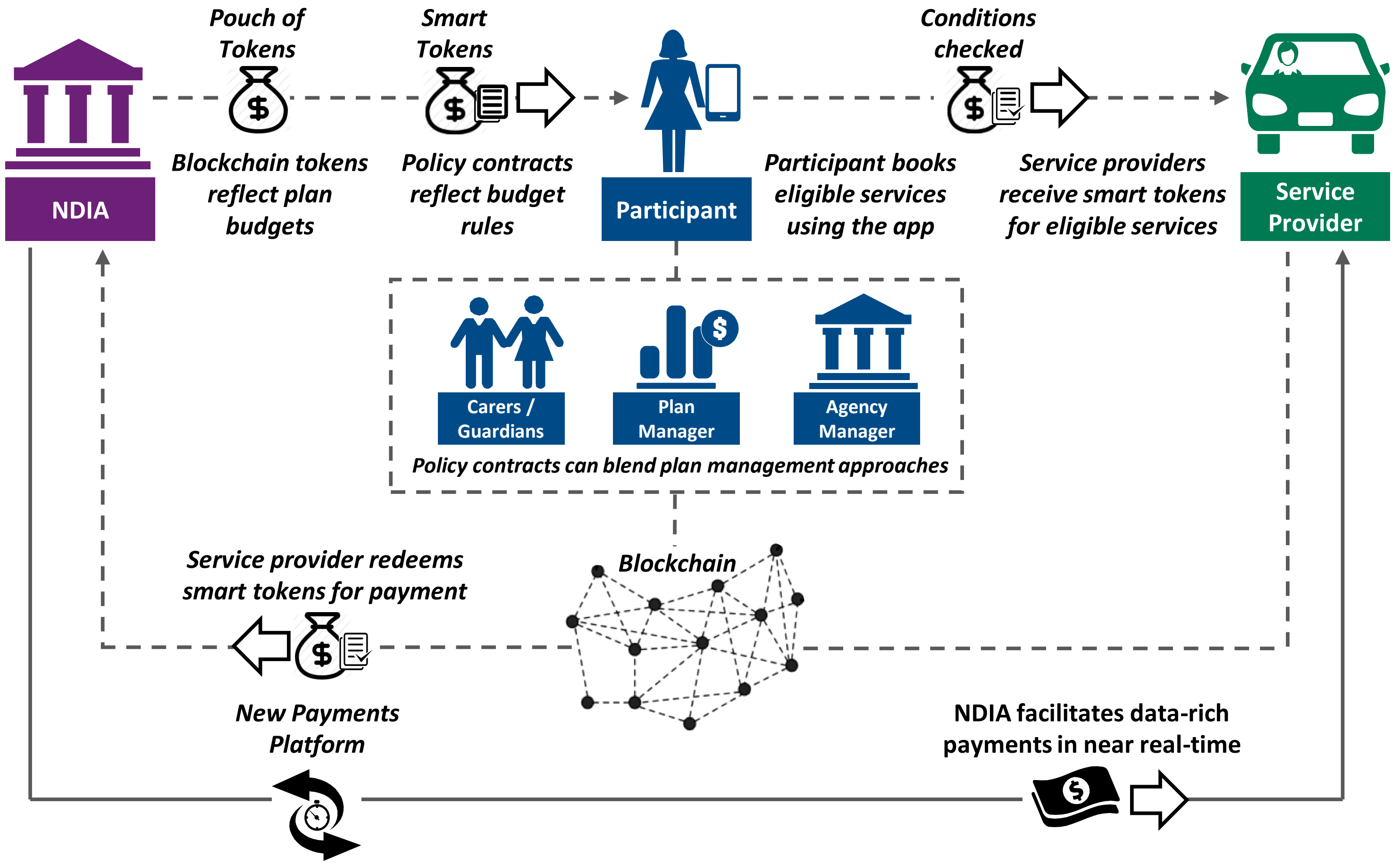
Friends of the Lab

**41**

people across CSIRO’s Data61 and the Commonwealth Bank

CSIRO DATA 61

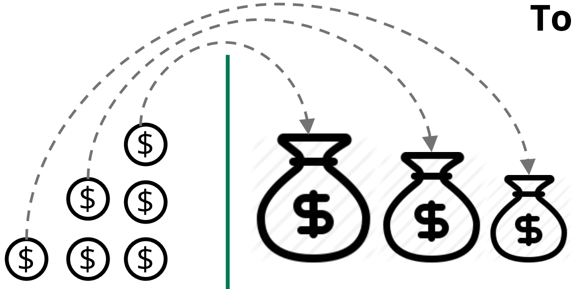
# Our proof of concept



Pouch of Tokens
Smart Tokens
Conditions checked
NDIA
Blockchain tokens reflect plan budgets
Policy contracts reflect budget rules
Participant
Participant books eligible services using the app
Service providers receive smart tokens for eligible services
Service Provider
Carers / Guardians
Plan Manager
Agency Manager
Policy contracts can blend plan management approaches
Service provider redeems smart tokens for payment
Blockchain
New Payments Platform
NDIA facilitates data-rich payments in near real-time

# How we make the money smart

## Tokens and Contracts



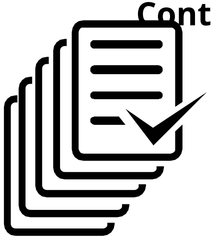
**Tokens** represent value of AUD for NDIS purchases.

**Pouches** represent different quantities of tokens.

**Policy contracts** give rules and enforcements (e.g. ownership, eligible services, nominations…)

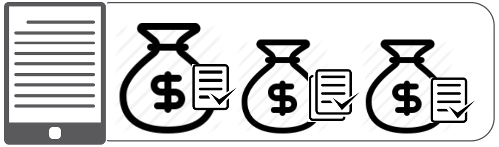
**Smart tokens** are formed when policy contracts are attached. Policies can be destroyed when not required (e.g. after payment).

## Provider Registry Contract



Providers are listed on a registry smart contract.

## Participant plans



Participant plans have pouches of smart tokens for each budget, which can be spent on services.

## Service Agreement Contracts

Service agreements can attach tokens to providers and enable payments as services are delivered.

# Making Money Smart

## The potential of Smart Money explained

Fahima tracks her budget progress, sometimes across multiple categories and payment stages.

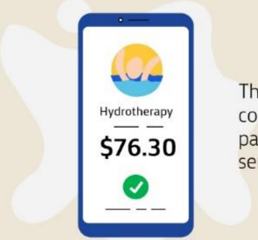
### Checking budget

$
$2,473.21
$839.72
$1,526.31

The Smart Money system could automatically keep track of all budget information in one place.

Fahima seeks NDIS funding for each service and pays from her own bank account.

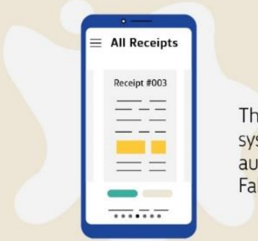
### Paying for services



The Smart Money system could enable automatic payments directly to the service provider.

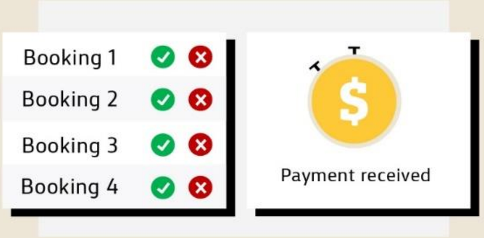
Fahima files her payment receipts for her records and potential plan audits.

### Keeping records



The Smart Money system could automatically log Fahima's receipts

## Service provider



The Smart Money system could confirm bookings and service eligibility in real-time.

The Smart Money system could enable payments within seconds and automatic reconciliation.

## Government

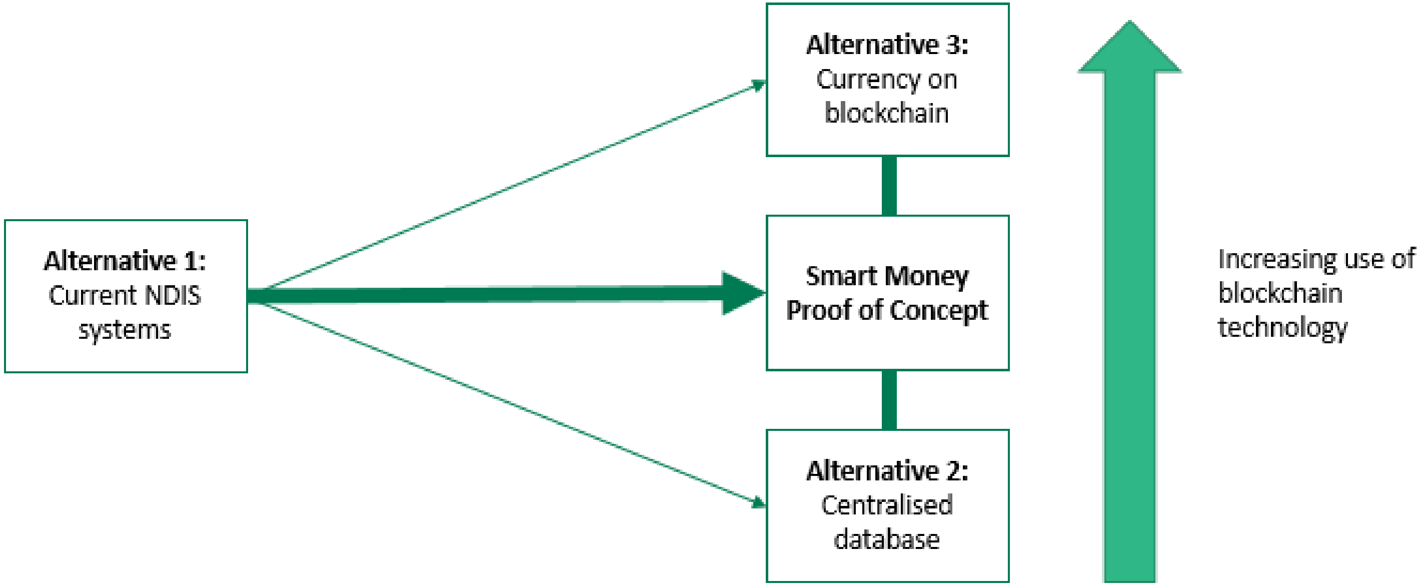
The Smart Money system could help ensure Fahima's plan activities support her goals, with appropriate privacy controls.

The Smart Money system could automatically confirm spending integrity without manual audit processes.

# We evaluated our proof of concept against 10 criteria

| Design Criteria | The Proof of Concept |
|---|---|
| 1. Choice | Potential of participants to make informed decisions about the services they access |
| 2. Control | Potential of participants to take control of their plans and delegate control as they choose |
| 3. Accessibility | Accessible to participants regardless of disability and all types of service providers |
| 4. Simplicity | Simple payments for participants, carers, plan managers, service providers and government |
| 5. Efficiency | Admin time and costs for participants, plan managers, service providers and government |
| 6. Confidentiality | Ensures the confidentiality of personal and commercially sensitive information |
| 7. Integrity | Ensures funds are spent as intended and enables government to identify potential mis-spend |
| 8. Performance | Achieves low latency, sufficient throughput and real-time payments |
| 9. Cost | Can be implemented and maintained at low cost |
| 10. Modifiability | Can accommodate changes in policy and be used in many conditional payment environments |

# We evaluated proof of concept against alternative options



**Alternative 1:** Current NDIS systems

**Alternative 3:** Currency on blockchain

**Smart Money Proof of Concept**

**Alternative 2:** Centralised database

Increasing use of blockchain technology

# We found the new solution options would deliver similar front-end benefits, with interesting back-end trade-offs

| Design Criteria | Comparative evaluation |
|---|---|
| 1. Choice | Smart Money = Currency-on-blockchain = Centralised database > Current NDIS systems |
| 2. Control | |
| 3. Accessibility | |
| 4. Simplicity | |
| 5. Efficiency | |
| 6. Confidentiality | Smart Money ≠ Currency-on-blockchain ≠ Centralised database > Current NDIS systems |
| 7. Integrity | |
| 8. Performance | |
| 9. Cost | |
| 10. Modifiability | |

| Design Criteria | Proof of concept vs Centralised Database Solution |
|---|---|
| Confidentiality | ➕ Anonymising the data held on blockchain through different private keys for each budget category to reduce extent of data leakage and re-identification |
| | ➖ Due to multiple nodes (in blockchain), POC would have a greater area for attacks |
| Integrity | ➕ Data stored on blockchain is immutable and transactions are validated by all nodes, making it difficult to manipulate data and so reducing risks of internal fraud |
| Performance | ⊜ Similar latency and throughput for an NDIS use case, and also similar speed of payments (as both would make payments on the NPP) |
| | ➖ Based on current blockchain technology, latency and throughput performance of POC would be lower if applied across multiple payment environments |
| Cost | ➕ Less expensive if applied (shared) across multiple payment environments |
| | ➖ More expensive if only implemented for the NDIS |
| Modifiability | ➕ Dynamic policy contracts likely easier to modify than rules in a centralised DB |
| | ➖ An immutable ledger and multiple nodes can make it more difficult to update the system, if changes to the underlying architecture are required |

| Design Criteria | POC vs Currency-on-Blockchain Solution |
|---|---|
| Confidentiality | ⊕ Currency-on-blockchain solution would involve the highest level of risk, as the attack surface area would be greatest and the value of breaching the solution would be higher (not just data, also currency). |
| Integrity | ⊜ Both solutions would reduce the incidence of ineligible transactions. |
| Performance | ⊕ POC would be faster as currency-on-blockchain solution would likely require a slower consensus algorithm for validating transactions.<br>⊖ Currency-on-blockchain solution would enable payment on-chain, eliminating the time required for NPP integrated payments. |
| Cost | ⊕ POC would be less expensive than a currency-on-blockchain solution to establish.<br>⊖ POC may be more expensive over the longer term as a currency-on-blockchain solution may would have wider application across the economy and therefore could spread costs. |
| Modifiability | ⊕ Currency-on-blockchain solution would likely involve a greater array of nodes and payment environments, which could make changes to the underlying architecture and creation of new policy contracts, more complex. |

# Concluding Thoughts

# What Is Blockchain/DLT Good For?

- Trustworthy and efficient ways to work together
  - Focus on spaces between individuals, organisations
  - Data integrity for information sharing
  - Neutral ground for process coordination

- Representing & controlling Digital Assets
  - (Especially blockchains)
  - Allows exclusive control over cryptocurrency, tokens

# Neutral Ground, Potential for Impact

- Choose your architecture to match your target NFPs
  - Key challenges for blockchain are Confidentiality, Performance
  - Key opportunities are Integrity, Availability

- Creates new options for design of systems and society
  - A common view of data, with no central controller
  - Logically-centralised data, administratively-decentralised control
  - Benefits from cost reduction and from innovation
    - Reduce cost & time of red tape, reconciliation, audit, dispute resolution
    - Inter-organisational drivers of productivity

# Thank you

**Data61**
Dr Mark Staples