final report

Project code:	V.DIG.0009
Prepared by:	Lawrence Parsons Unico Computer Systems Pty Ltd
Date published:	31 July 2018

PUBLISHED BY
Meat and Livestock Australia Limited
Locked Bag 1961
NORTH SYDNEY NSW 2059

Evaluation of Blockchain Technology to deliver industry integrity programs

Meat & Livestock Australia acknowledges the matching funds provided by the Australian Government to support the research and development detailed in this publication.

This publication is published by Meat & Livestock Australia Limited ABN 39 081 678 364 (MLA). Care is taken to ensure the accuracy of the information contained in this publication. However MLA cannot accept responsibility for the accuracy or completeness of the information or opinions contained in the publication. You should make your own enquiries before making decisions concerning your interests.

Abstract

A wholly owned subsidiary of Meat & Livestock Australia, the Integrity Systems Company (ISC) is responsible for delivering the red meat industry's on-farm assurance and through-chain traceability programs. These are the Livestock Production Assurance (LPA) program, the National Vendor Declarations (NVD) and the National Livestock Identification System (NLIS) which together make up Australia's red meat integrity system.

Via a couple of research projects ISC is investigating how Blockchain might be applied within industry integrity systems to identify potential benefits and challenges of this technology. UNICO was engaged specifically to identify if Blockchain had the potential to improve the integrity of the National Livestock Identification System (NLIS) Mirror database currently maintained by ISC and provided to the State and Territory Governments of Australia via the aggregated State databases.

The service ISC provides to members in the NLIS database, supports the Australian Red Meat industry in the identification and traceability of cattle, sheep and goats. Amongst other details, it captures the movement of animals by using electronic RFID tags or visual tags. This database is of vital importance to the Red Meat Industry.

ISC is looking for feasible Blockchain solutions to address current issues, challenges and gaps associated with the NLIS database and associated interfacing components such as Mirror database and individual State databases.

This final report reviews the current processes and provides an overview of the current NLIS database and its replication to the States via the Mirror Database, highlighting potential benefits and challenges of utilising Blockchain technology to mitigate current challenges for ISC.

Executive summary

> "*Now, in the hyper-connected and ever evolving world, transparency is the new power*"
> *-Benjamin Herzberg, Program Lead, Private Sector Engagement for Good Governance at the World Bank Institute*

Blockchain technology is maturing and is primed to alter data transactions conducted between third-parties to be fundamentally altered. The business fit for blockchain is seemingly endless, as such Integrity System Company (ISC) commissioned an investigation into how and where a blockchain distributed ledger solution could fit into the Mirror Database aggregation of the main National Livestock Identification System (NLIS) database and the sharing of data with the States and Territories within Australia.

This report discusses the results of this investigation and addresses the potential advantages and limitations of the technology to assist in the identified issues and concerns with the current data synchronisation procedures and infrastructure.

First, the report investigates the current aggregation process of the Mirror database and the synchronisation of it to the State Database in each State and Territory. **The objective is to identify an application of Blockchain technology that could improve on the current identified concerns in the present solution of data aggregation and synchronisation between the Mirror database and State database.**

The report then explores potential solutions to the identified concerns raised, discusses the advantages and disadvantages of each one, finally culminating into a recommended solution and a proposed approach to the implementation thereof.

> *"The practical consequence […is…] for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate."*
> - Marc Andreessen, Inventor of the internet browser

Blockchain has the potential to reinvent and remove some key business restrictions throughout the digital world as data moves from one participant to another, thus, enabling greater trust and security to how each party interacts and transacts across the extended supply chain.

The benefits of creating a more trusted data source for the Red meat industry, when considering the Mirror database and State database and the role it plays in governance and compliance, to the well-established regulations that protect the livestock in Australia cannot be over-stated. This extends to consumers of the products produced and producers of red meat. This report illustrates how this can be achieved and how transparency can be achieved.

Table of contents

1 Project Background

A Blockchain is a form of distributed ledger technology (DLT) that connects different parties over the internet to provide a secure and trustworthy record of transactions (both financial and non-financial), without giving control to a third party. A Blockchain solution by its design proves the source and integrity of information contained in it. This means it has the potential to open new ways of delivering industry integrity programs along existing supply chains, as well as ensuring the provenance of products internationally.

There is currently a lot of hype around Blockchain technology and there is significant investment occurring internationally. In Australia there is also a great deal of activity, however most is still at the research and development stage with little to no commercial activity at present. Given the typical adoption timeframes of the Australian red meat industry and the potential transformational nature of this technology, it is important that we commence investigative work in this area to review potential applications and benefits for the red meat industry in Australia.

Integrity Systems Company (ISC) (a wholly own subsidiary of MLA) identified that Blockchain technology had the potential to improve integrity systems for the Australian red meat industry. ISC was interested in investigating how Blockchain might be applied within industry integrity systems to identify potential benefits and challenges of this technology.

The purpose of this project was to look at whether Blockchain technology offers any advantages for MLA/ISC in how industry integrity programs are managed (i.e. a decentralised model over a centralised model), with specific focus on the Mirror database.

2 Project objectives

- Explore and report on how using a blockchain based database, the National Livestock Identification System (NLIS), Mirror database could be synchronised across the various states to ensure integrity and traceability of data records.
- Examine the use of the block chain across the NLIS Mirror database and opportunities to use the blockchain distributed data characteristics to improve synchronising, preserving and enhancing data integrity.
- Explore how blockchain can be applied to the NLIS Mirror database to synchronise using distributed database concepts.
- The report will propose how a blockchain distributed database solution could be applied to verify the integrity of data.

3 Methodology

To understand how the NLIS Mirror database operates, how it is created and then aggregated to the different States and Territories Government authorities; a series of investigative tasks were undertaken. These are discussed in more detail below.

Detailed activities

3.1 Site visit to MLA Head Office

The first activity involved gaining an understanding of the way the NLIS database is aggregated into the NLIS Mirror database. Included in this activity was understanding the constraints and issues faced by ISC in the maintenance and administration of the NLIS database along with the aggregation into the Mirror database. This encompassed the distribution of this database to the State database.

The focus and objective of these sessions were to clearly understand the existing pain points, bottlenecks and where possible, canvasing the reasons for decisions that have been made in the past.

The Mirror database, its architecture and components were investigated as part of the discovery. It is understood that the Mirror database contains information related to movement of animals such as location details where animals have moved from and current location.

Animal attributes, such as the recorded tags, assist in identifying animals uniquely. Other information such as quantity, breed, sex, killing information, animal status, carcase feedback, and some information around who has provided the information etc. is also recorded in the Mirror database.

Information is fed into the NLIS database by various parties such as farmers/producers, abattoirs/processors, feeders, buyers and agents who buy or collect livestock. The system facilitates third parties to comply with state regulations relating to biosecurity and traceability.

Each NLIS submission serves a distinct purpose (a file cannot be submitted/uploaded containing both cattle transfer and kill details, as example) and each file type is identified based on the uploaded value or submission location. This ensures the correct identification and processing of the data.

3.2 Site visit to State offices of the Victorian Department of Environment, Land, Water and Planning

A visit to the Victorian Department of Environment, Land, Water and Planning was undertaken to investigate the consumption of the Mirror database by the State and to identify current concerns and constraints.

The State of Victoria consumes the NLIS data for reporting purposes only. The reports generated are for the purposes of tracing livestock movements from registration to either feedlots or saleyards and then eventually to abattoirs.

The State of Victoria have built many add-on applications that consume the NLIS data to effectively monitor the compliance of the various entities along the red meat supply chain in Victoria.

The data generated from the database aids in the regular compliance auditing of saleyards, abattoirs and producers.

4 As Is

4.1 Current Systems

As mentioned, the NLIS database is currently aggregated into the Mirror database which is then synchronised to the individual State and Territory databases.

4.1.1 Mirror Database

The Mirror database is where NLIS data is stored in an aggregated form, hence the number of tables and columns are less when compared to the full NLIS dataset. Currently, the Mirror database has approximately 25 tables and contains enough information to record the required details relating to animal movements, killing information, etc.

The Mirror database is the “master” for the databases in each State and Territory (State database). As this is the current system by which states can access the NLIS data and Mirror database acts as a source of truth for State database.

4.1.2 State Databases

The State database are maintained by each State and Territory government.

This database is owned by the respective States and Territories. Each State or Territory is provided with an NLIS feed using Microsoft’s incremental one-way pull merge replication.

5 To Be

5.1 What is Blockchain

Blockchain is a decentralised, distributed ledger technology. It provides for the creation, validation and encryption of digital transactions and record them in an immutable way. – Forbes 2018

It is a database of groups of transactions (blocks) that are linked to a previous group of transactions (the chain) and is replicated and distributed to all node participants in the network so that all copies of the database are identical. Blockchain records every transaction that happens and is immutable.

A distributed ledger is a type of database that is shared, replicated, and synchronised among the participants/members of a network.

The distributed ledger records transactions, such as the exchange of assets or data, among the participants in the network. Participants in the network govern and agree by consensus on the updates to the records in the ledger. No central, third-party mediator, such as a financial institution or clearinghouse, is involved. Every record in the distributed ledger has a timestamp and unique cryptographic signature, thus making the ledger an auditable history of all transactions performed in the network.

In short, a blockchain can be described as a network of computers, each having an identical copy of the database (distributed) and changing its state (records) by common agreement based on an algorithm, with no need for any central server or agent.

- Blockchain technology can be used in a private or public peer-to-peer network of parties, who all participate in a given transaction. The technology uses a distributed ledger that is visible to all participants involved in the transaction. Through a consensus mechanism, the ledger is guaranteed to be consistent. Because the ledger is distributed, everyone involved can see the “world state” at any point in time and can monitor the progress of the transaction. By its very nature, blockchain can tackle the following business issues: Trust – Through the use of blockchain, all the parties involved in a transaction only must trust the blockchain without a need for a central intermediary;
- Transparency – Because the ledger is distributed, all peers involved in the transaction network can view it subject to security rights (private blockchain);
- Accountability – Since all parties in the transaction can view the distributed ledger, everyone can agree on how the transaction is progressing while it is ongoing, and how it went once it is complete.

So, to summarise, blockchains are:

1. Transaction ledgers

2. Immutable
3. Consensus-driven
4. Decentralised
5. Trust less (it's not based on a system of trust)
6. Secured by cryptography
7. Can be made public

5.1.1 What is a smart contract?

A smart contract is a piece of code stored in the blockchain network (on each participant database). It defines the conditions on which all parties using the contract agree and certain actions described in the contract can be executed if the required conditions are met. As the smart contract is stored on every computer in the network, they all must execute it and get to the same result. This way users can be sure, that outcome is correct.

5.1.2 A typical blockchain transaction works broadly as follows:

i. Transaction initiation: One party (the sender) creates a transaction and transmits it to the network. The transaction message includes details of the receiver's public address, the value of the transaction, and a cryptographic digital signature that proves the authenticity of the transaction.

ii. Transaction authentication: The nodes (computers and users) of the peer network receive the message and authenticate its validity by decrypting the digital signature. The authenticated transaction is placed in a "pool" of pending transactions.

iii. Block creation: Pending transactions are put together in an updated version of the ledger, called a block, by one of the nodes in the network. At a specific timing interval, the node broadcasts the block to the network for validation

iv. Block validation: The validator nodes of the network receive the proposed block and work to validate it through an iterative process that requires consensus from most of the network. Because all parties have the same data set, they validate by ensuring the information matches their ledgers. Given that the validation happens across multiple peers in the network that compare the information to their own data sets, fraudulent transactions are nearly impossible.

v. Block chaining: If all transactions are validated, the new block is "chained" into the blockchain, and the new current state of the ledger is broadcast to the network. This whole process can be completed within 3 to 15 seconds or even faster as the technology advances.

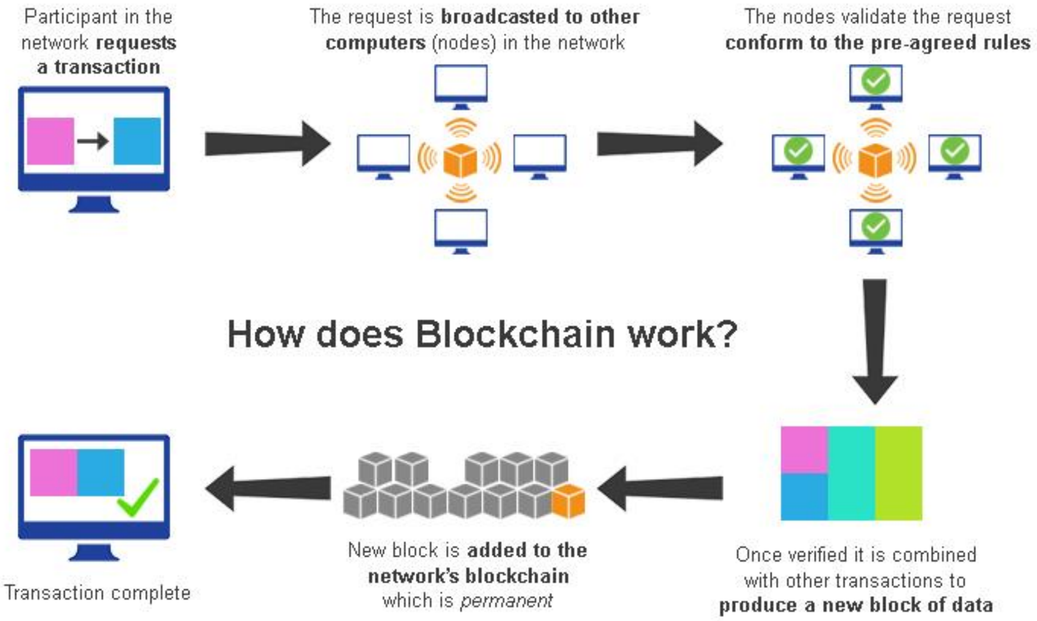

Participant in the network requests a transaction
The request is broadcasted to other computers (nodes) in the network
The nodes validate the request conform to the pre-agreed rules
How does Blockchain work?
Once verified it is combined with other transactions to produce a new block of data
New block is added to the network's blockchain which is permanent
Transaction complete

FIGURE 1 – A typical blockchain transaction. Source: http://netsend.com/blog/introduction-to-blockchain-technology/attachment/introduction-to-blockchain-technology/

5.1.3 Public Blockchains

Public blockchains, such as Ethereum and Bitcoin, are blockchains which are accessible by anyone. An individual can access either blockchain and enter transactions using the blockchain. In addition to being open access, all the data on public blockchains is public. Anyone can access these blockchains to see a flow of transactions if they wish to.

Advantages:

Autonomy
Autonomy is an advantage of a public blockchain in that no one individual or company can control the information which is contained on the blockchain or the rules governing the blockchain. It is not possible for the “owner” of the blockchain to change the rules of the blockchain. The information about the transactions is authenticated by means of an agreement between the users of the blockchain. Thus, the users of a public blockchain do not have to place their trust in a third party to use the blockchain. Instead, a user of a public blockchain can trust the blockchain itself.

Security out of publicity

Although it is possible to hide the actual identity of all associated participants on blockchains, all data on public blockchains is public. The security is obtained by their very publicity, where every participant can see all account balances and the info regarding all transactions.

Availability

Bitcoin, Ethereum, Hyperledger and other public blockchains were created to be available by anyone having a computer and access to the internet.

Disadvantages:

Disadvantages of public blockchains include lack of speed and the inability to control access to data.

5.1.4 Private Blockchains

In contrast to public blockchains, private blockchains are blockchains which are operated by an organisation or consortium of organisations and which are only accessible to individuals or organisations which have been granted permission to use the blockchain by its operator. Private blockchains are essentially private databases which are structured as a distributed ledger.

For some companies, the private nature of a private blockchain is a key advantage, as it maintains the confidentiality of information concerning transactions made on the blockchain and prevents commercially sensitive information from being viewed by anyone with access to the internet.

Advantages:

The transaction speeds

The transaction speed of a private blockchain is generally faster than public blockchain. The speed can even be the same with the speed of a normal database that is not a blockchain. This is because there are not many cross-points all with high trust levels. There is no need for every cross-point to verify a transaction. For example, it takes upwards of 10 minutes for the Bitcoin blockchain to confirm transactions, whereas private blockchains are likely to have significantly quicker confirmation times as less data must be processed and transferred for transactions to be validated.

Cost of transactions

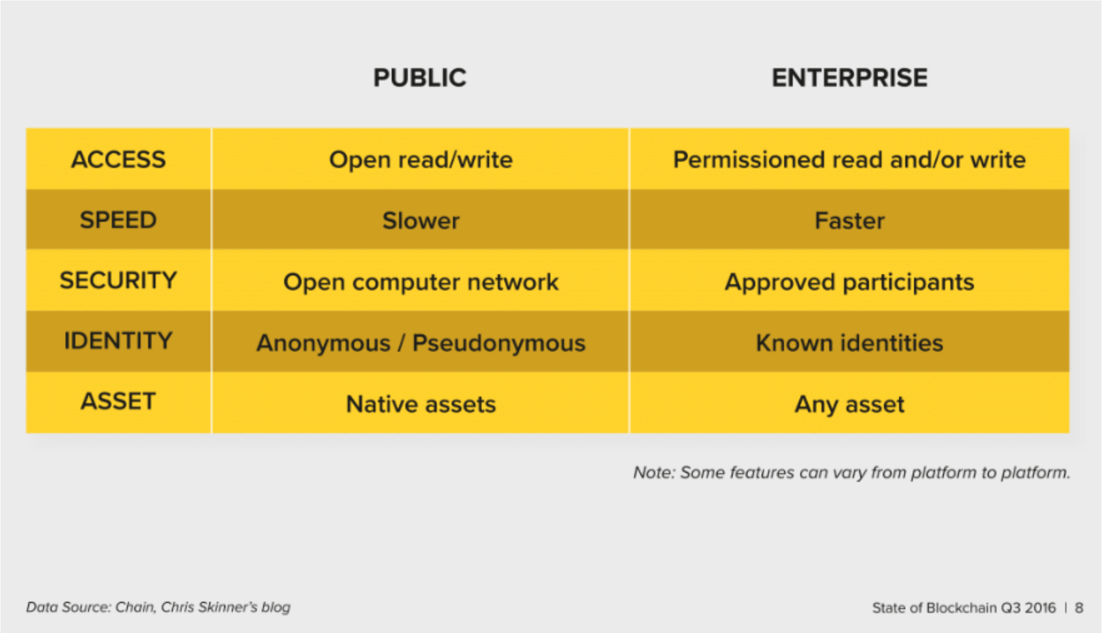
The cost of transactions in private blockchains are generally not very expensive, they can even be free. If a company oversees all transactions and processes, it does not need to change the cost of work, even if the transaction is processed by multiple entities, such as competing banks. The transaction fees can still be very small for the same reasons that they can be so fast. Complete agreement between nodes isn’t required, so fewer nodes need to do the work for any one transaction.

Disadvantages:

Flexibility

If such a need arises, a company running a private blockchain can easily change the rules of a Blockchain, revert transactions, modify balances, etc. Of course, one can argue that one can do this on a public blockchain by giving the government a backdoor key to a contract.

The differences between a public and private (enterprise) Blockchain can be summarised as below.



	PUBLIC	ENTERPRISE
ACCESS	Open read/write	Permissioned read and/or write
SPEED	Slower	Faster
SECURITY	Open computer network	Approved participants
IDENTITY	Anonymous / Pseudonymous	Known identities
ASSET	Native assets	Any asset

Note: Some features can vary from platform to platform.

Data Source: Chain, Chris Skinner's blog

State of Blockchain Q3 2016 I 8

Figure 2: Table comparison of Private and Public Blockchains. Source: https://www.coindesk.com/research/state-of-blockchain-q3-2016/?slide=8

5.2 Potential Solution

It is recommended that a Blockchain solution be implemented. This approach however, does have advantages and disadvantages.

ISC is dedicated to and engaged in on-going works, targeting current issues identified during the initial phases of the project.

5.2.1 Incremental Blockchain solution

The entire NLIS Mirror database could be replaced using a Blockchain technology solution. Due to the sheer volume of transactions and transaction options available to a user of the Mirror database, this approach is best divided up into defined milestones and tasks. This would ultimately end with the replacement of the current Mirror system and database with a private Blockchain.

Using a private Blockchain is recommended as the requirement to assign roles is important to secure sensitive information from unauthorised access.

As the Mirror database contains many tables and features, it is possible to approach such a change on an incremental basis.

Advantages of an "Incremental blockchain" solution

1. Changes can be made incrementally hence there are minimal risks that would affect the availability of the Mirror database;
    - The ISC and States can incrementally increase their capabilities such as integration, application refactoring, maintenance and support.
    - Receive early feedback from states and adjust accordingly.
2. Benefits of using blockchain for NLIS Mirror database
    - Enhancing the integrity of the NLIS Mirror data.

  - This is achieved by each State being a "verification node" in the blockchain, giving them "voting" rights on new data being inserted into the blockchain ensuring the validity of new records and amendments to existing records.
- Enhanced consistency of data between States and Territories
  - With each State and Territory being a "node", each have identical versions of the Mirror database.
- Local API's and connectivity to the chain (Loopback API)

  E.g.: Hyperledger Composer can be integrated with existing systems by using a Loopback API. Integrating existing systems allows connections to pull data from existing business systems and convert it to assets or participants in a Composer business network
- Open new opportunities to support other features, including a full blockchain network for the industry

Disadvantages of an "Incremental blockchain" solution

1. Requires a significant investment to achieve.
2. Co-ordination of acceptance by all States and Territories.
3. Smaller States may not have enough budget.
4. Some states or territories may not have the required skill-sets amongst staff, leading to further expenditure (e.g. Training)

There are two distinct phases of this proposed solution. The first is to deal with the current consumption of data by the States and Territories, the second is to deal with any future consumption requirements of the NLIS data.

Addressing the current consumption requirements

At present the States and Territories have local copies of the Mirror database, referred to as State databases. Each State and Territory have also created numerous reports to analyse the compliance of traders, sale yards and abattoirs etc. to local laws and regulations. The Victorian Department of Environment, Land, Water and Planning further extract and aggregate the data to generate reports. To minimise disruption of current processes and reduce risk, this approach would extract the required data from the Blockchain via a "data pump" into the local State database on a regular interval, allowing current reports to operate without the need for modification. This approach is illustrated in the diagram below. It is desirable that these reports eventually extract the data directly from the Blockchain as it is immutable, where a State database could more easily be changed.

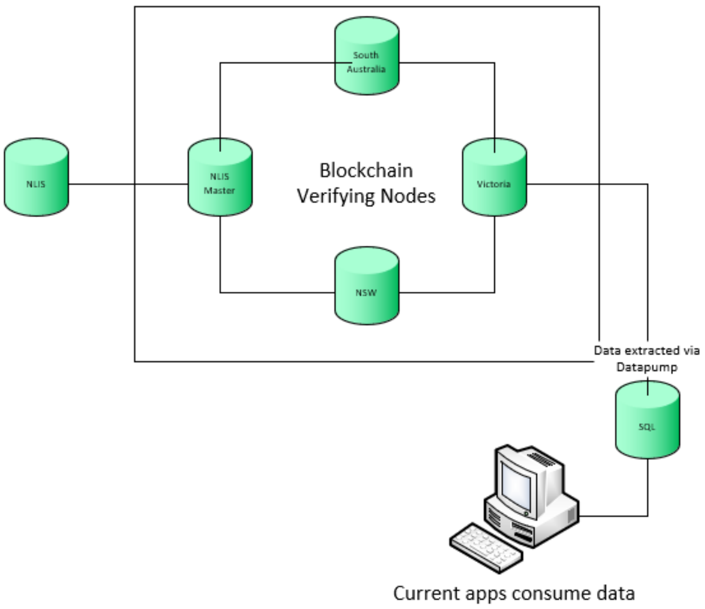

South Australia
NLIS
NLIS Master
Blockchain Verifying Nodes
Victoria
NSW
Data extracted via Datapump
SQL
Current apps consume data

Figure 3: What a potential "Incremental blockchain" approach could look like for <u>current</u> applications that consume the State database data.

Addressing potential future consumption requirements

Any future reports or data extract required would now be able to be achieved with a direct connection to the Blockchain via an API. This is illustrated in figure 3.

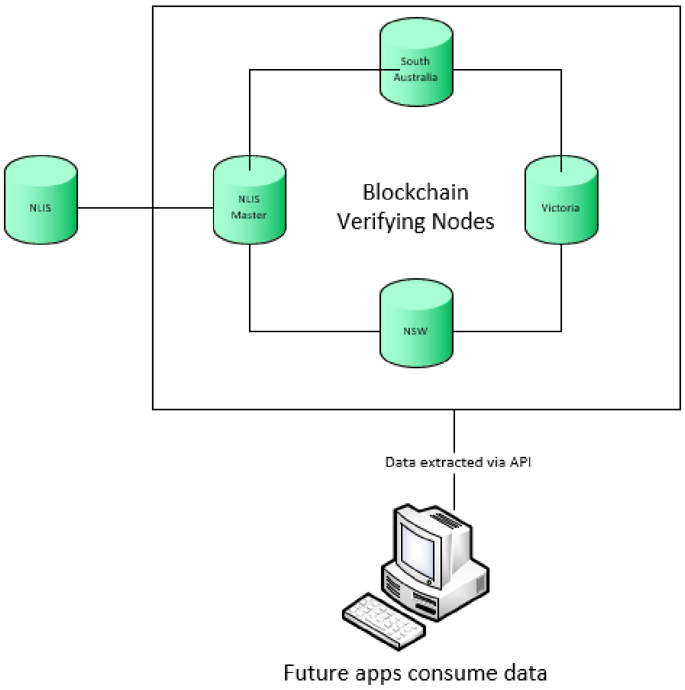


Figure 4: What a potential "Incremental blockchain" approach could look like for <u>future</u> applications that consume the State database data.

6 Conclusions/recommendations

6.1 Potential solution (Incremental) Roadmap

This option would involve an incremental approach to moving the entire NLIS Mirror database to a Blockchain solution. To be successful in such a large undertaking an incremental approach would be advisable and each “function” within the NLIS Mirror database will be transformed as a part of the overall project of replacing the distributed Mirror and State databases. Functions in this context refer to PIC Information management, animal movements, kill information etc.

To minimise disruption of current processes and reduce risk, this approach would extract the required data from the Blockchain via a “data pump” into the local State database on a regular interval, allowing current reports to operate without the need for modification.

By way of example, the “Movement of Animals” feature of the NLIS Mirror database would be moved to a Blockchain. This data would contain NLIS Tag numbers and/or RFID details, as well as information relating to the properties the animal was moved from and to. As this information is in a Blockchain, an API would need to be created that would allow State database users to connect to this relocated dataset. Therefore, the only change that would be required to existing reports on the part of the State Authorities would be the location of the dataset that is used to generate the report on animal movements.

It is recommended that these reports extract the data directly via an API attached to the Blockchain as it is immutable, where a State database could potentially be changed.

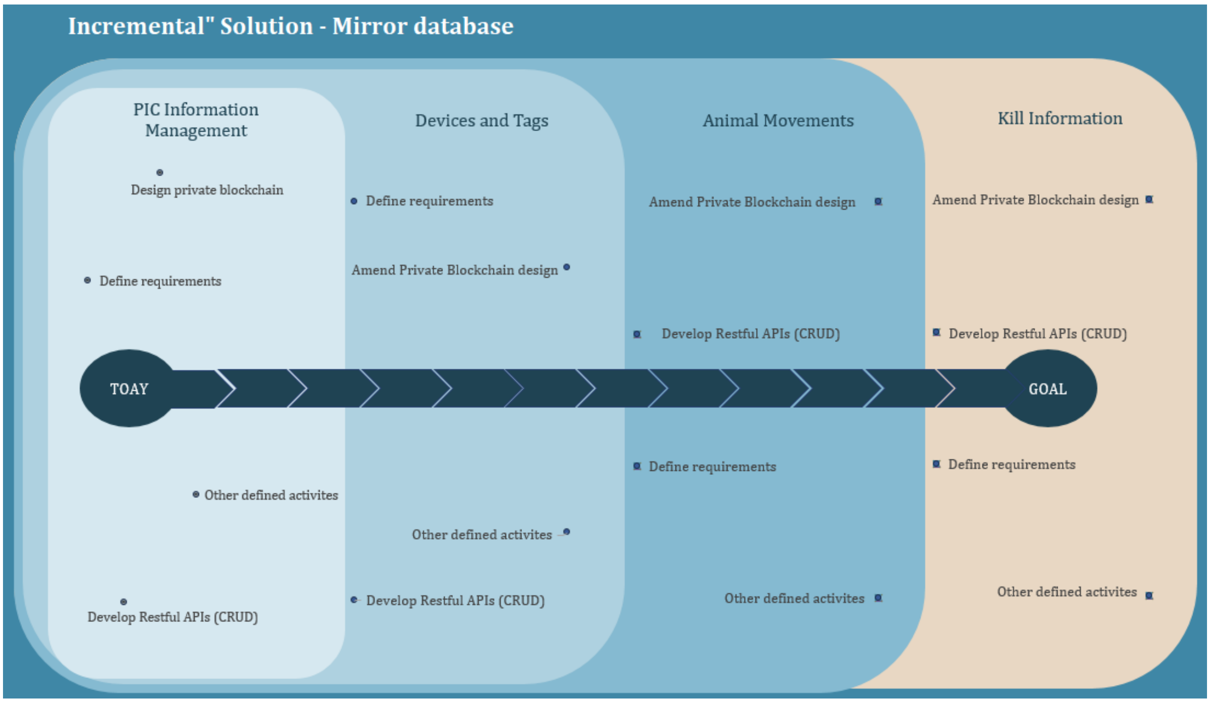

Incremental" Solution - Mirror database
PIC Information Management
Design private blockchain
Define requirements
Other defined activites
Develop Restful APIs (CRUD)
Devices and Tags
Define requirements
Amend Private Blockchain design
Other defined activites
Develop Restful APIs (CRUD)
Animal Movements
Amend Private Blockchain design
Develop Restful APIs (CRUD)
Define requirements
Other defined activites
Kill Information
Amend Private Blockchain design
Develop Restful APIs (CRUD)
Define requirements
Other defined activites
TOAY
GOAL

Figure 5: What a potential “Incremental blockchain” approach roadmap would look like.

7 Considerations

Some important points need to be considered and resolved for a Blockchain solution to be effective. Please refer to the considerations below.

7.1 Development of a Blockchain strategy

As the business problems were discussed and identified the benefit that blockchain can address these for the Mirror database were highlighted. As such it is of paramount importance to success, that a detailed strategy be developed and potentially developing a proof-of-concept is a prudent approach.

7.2 Selecting a Blockchain platform

The future direction of the blockchain ecosystem remains unclear, we believe that private blockchain, also referred to as a permissioned Blockchain is the best option for the Mirror database as ISC and the States can tailor the standards to their specific legal frameworks and requirements.

Over time, it is likely that a public blockchain networks and hybrid model (a combination of aspects from public and private networks) are likely to be developed as certain data can be exposed to other parties in the value chain, abattoirs being an example.

The benefit of a hybrid model, would allow for the sharing of “public” domain information in the public portion of the blockchain, an example of this might be NLIS tag data and information.

More sensitive information could be stored in a Permissioned Blockchain, examples of which include transactional data and industry sensitive information, in the form of movement data etc.

7.3 Closing the talent gap

ISC and the State and Territory authorities will need to develop or acquire additional skills and expertise to succeed with blockchain. Blockchain is a relatively new technology so underestimating the talent challenge would be ill-informed. We would recommend additional blockchain skills in areas such as Public Key Infrastructure (PKI), cryptography, information architecture, software engineering, network infrastructure and integration, and user interface/user experience.

7.4 Overcoming external roadblocks

Privacy and security are issues central to blockchain adoption. Regarding privacy, permissioned blockchain networks are configurable, in that they would allow enterprise users to limit access to their data.

Legal and regulatory issues are also potential obstacles to the adoption by the States and Territories, so these concerns would need to be adequately addressed.

8 Bibliography

Tapscott, Don, and Alex Tapscott. *Blockchain Revolution How the Technology behind Bitcoin Is Changing Money, Business and the World*. Portfolio Penguin, 2016.

https://www.forbes.com/sites/forbesagencycouncil/2018/04/05/what-is-blockchain-and-what-can-businesses-benefit-from-it/#5845eb64675f

Iinuma, Arthur. "What Is Blockchain And What Can Businesses Benefit From It?" Forbes, Forbes Magazine, 5 Apr. 2018, www.forbes.com/sites/forbesagencycouncil/2018/04/05/what-is-blockchain-and-what-can-businesses-benefit-from-it/.

"Integrating Existing Systems." Hyperledger Composer - Create Business Networks and Blockchain Applications Quickly for Hyperledger | Hyperledger Composer, hyperledger.github.io/composer/latest/integrating/integrating-index.https://www.coindesk.com/research/state-of-blockchain-q3-2016/?slide=8

Herzberg, Benjamin. "The Next Frontier for Open Data: An Open Private Sector." Governance for Development, 25 Mar. 2014, blogs.worldbank.org/voices/next-frontier-open-data-open-private-sector.
Plant Biosecurity Act 2010 No. 60 of 2010 (Victoria)

"Blockchain: the Solution for Supply Chain Transparency." Provenance, Project Provenance Ltd, 21 Nov. 2015, www.provenance.org/whitepaper.

Meat & Livestock Australia (MLA, 2010) Mirror Database – Init & Synch Job Plan.doc

Meat & Livestock Australia (MLA, 2010) Mirror Database – Init & Sync Design Document.doc