U-Reg

Digital Identity Vault for Self-Sovereign Corporate Identity

November 2020

Authors: U-Reg Pte. Ltd.
www.u-reg.com

Contents

This Whitepaper aims to discuss how a distributed solution that allows to efficiently exchange regulatory documents would help simplify KYC processes, improve client experience and reduce costs.

All market participants agree that the financial industry cannot compromise with the AML and CFT requirements issued by regulators, in the case of Singapore by the MAS. At the same time KYC processes have been and remain a significant problem for the financial industry. They are costly, time consuming and cumbersome, for all parties involved. There has been a number of project that have tried to bring a solution, generally geared towards harmonization as a way to solve the problem. However most of these attempts have failed to deliver a durable solution.

U-Reg's proposed solution aims to tackle the KYC problem differently, by focusing on a single problem at a time rather than targeting a full harmonized KYC passport. Any attempt to solve the KYC problem must start with an efficient document collection process, which is today bilateral and repetitive. We believe that solving the problem around the collection, management and storage of documents needed for KYC analysis is the first necessary step to solve the broader problem around KYC workflows.

It was also established that the end-state of this project would be to plan for a transition from a centralized to a decentralized state, i.e. to use blockchain technology to facilitate the exchange of regulatory data or documents on a distributed ledger, with both architectures working in parallel. A distributed ledger brings additional benefits with regards to security and integrity of the underlying data. At the same time, we anticipated that a number of clients would not be able to adopt blockchain technology in the near future, hence the need to also build and maintain a classic architecture that would communicate with the distributed ledger, and vice versa.

To that effect, we have built a document repository that facilitates document exchanges between document providers and document recipients, and that eliminates or significantly diminishes the number of bilateral actions. It also significantly reduces time, resources and money spent on the sole document collection process. It is a true industry wide initiative that brings benefits across jurisdictions and across market participants.

We have also designed a private distributed ledger to enable the exchange of regulatory documents on a distributed network. We realized throughout the POC that a design presentation was not decisive enough to evaluate the adoption potential of the solution in the near future. We have therefore built a prototype of a distributed ledger to better assess the prospects for adoption and potential commercial application, two points that we are also discussing in this document for both the traditional architecture and for the distributed ledger.

a. Background

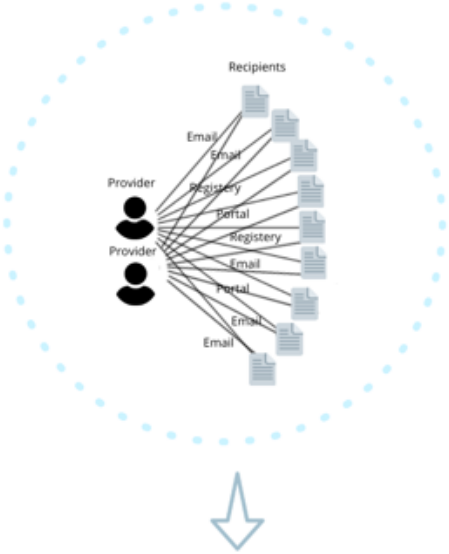
The KYC process remains an area of improvement for the financial industry despite large amount of resources allocated to solve this problem, including a number of initiatives focused on shared platforms or KYC utilities. These efforts have generally yielded limited results.

Past initiatives have often tried to deliver a full-fledged harmonized KYC solution, which is one of the reasons explaining the lack of results. Harmonization of KYC processes and requirements across jurisdictions or across banks for example seem very difficult to achieve in the medium-term, if at all.

b. Learning from past projects

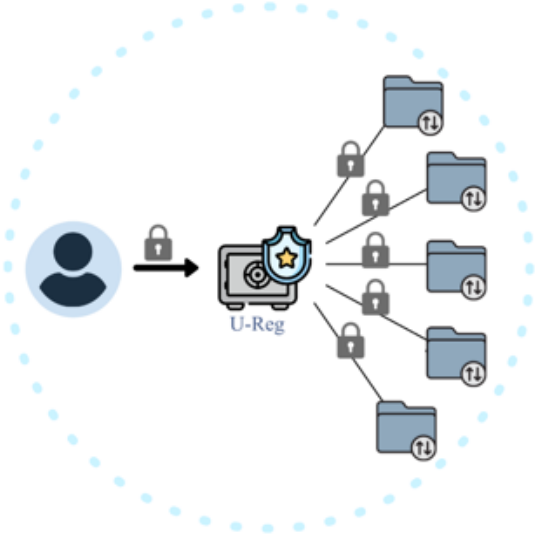
A number of solutions envisioned in the industry have assumed that a shared platform would instantly deliver a standard KYC process, which in turn would allow to mutualize analysis and KYC certifications. The knowledge sharing document published by the Associations of Banks in Singapore (ABS) on the project of a KYC utility in Singapore, first proposed in 2017, lists a number of reasons why establishing such utility is challenging.

We believe that a more gradual approach, focusing on a single problem and solving it well, rather than aim at a full standardized KYC, might allow to make one or two steps in the right direction.



c. Understanding Pain Points

As illustrated on the attached diagram, we would like to establish that the difficulty of KYC starts at the beginning of the process, during the document collection phase. The KYC document management life cycle is a web of bilateral interactions between documents providers and document recipients. The problem worsens when clients operate in multiple jurisdictions or have relationships with banks in different locations. Clients see the complexity increase further due to differing regulatory requirements in each country or to differing processes for providing documentation.



Worse still, document providers or clients, have to repeat this process with **all** their business relationships despite the fact that the documents needed are largely the same across institutions processing a KYC.

For example, a client onboarded by 10 banks would need to send the same documents 10 times throughout a year. This could then be multiplied by the number of jurisdictions or by the number of entities relevant to this relationship (for example, all relevant funds for an asset manager). This is time consuming, frustrating, cumbersome and costly.

Document providers, corporate or institutional clients, have generally made it clear that they would embrace a space where they can enter all of the necessary data one time, and where their banking partners can then tap into it as needed

d. Past and current solutions

The idea or a concept of a document vault applied to KYC processes is not new. Bloomberg and Refinitiv both exited the KYC utility market to focus on their core businesses while Markit and Swift have built KYC out-sourcing services that encompasses repository features. In the case of Swift this service is mainly used across banks, despite ongoing efforts to open it to corporate members too.

There are also service providers that propose document exchange or vault solutions. Dropbox would be a basic example, or again Virtual Data Rooms (VDRs) that some investment managers actually use to deposit KYC documents. However, these solutions are static and have not necessarily been built to dynamically manage the life cycle of regulatory documents. These solutions do not include updates on changes in circumstances, alerts on management of expiries, or non-standard requests for example, which are all paramount to KYC workflows. Furthermore, these solutions do not provide data extraction, data structuring or form filling capabilities, features that U-Reg has developed and is developing.

Finally, one could make a case, and rightly so, that MyInfo in Singapore or other one stop data platforms propose a large part of what would be needed in that space. However, MyInfo or other national solutions are at the same time fundamentally limited in scope. Not all documents required for a KYC analysis can be found on such platforms, especially not private documents. In addition, MyInfo is only relevant for a Singapore company processing a KYC on another incorporated Singapore company, assuming the latter has granted access to the former. This only represents a small fraction of the global needs.

e. Expected Benefits

A document vault utility that reduces significantly the number of bilateral actions between clients and FIs, if not eliminate them, brings a number of benefits.

Improve User Experience

Benefits of a repository where clients manage one single interaction are clear for document providers, but also for their recipients. A number of studies or market reports show the importance of client experience in the relationship. Surveys demonstrate that clients are more likely to change providers due to poor client experience.

Reduce Operational Risk

The ability for a recipient to tap into updated documents and forms allows for continuous KYC, and for a more efficient monitoring of changes in circumstance. The reduction in operational risk is further highlighted especially by the feature whereby a recipient is notified of any updates to the existing set of documents uploaded in the repository. This results in an increase of the data quality, and a better monitoring of a client's regulatory identity.

Reduce Costs

Reducing the number of interactions and automating processes help lower costs. Reducing operational risks, as discussed above, also contributes significantly to a reduction of costs such as one-off items linked to mistakes in input.

Accelerate Time to Market

A document vault utility helps accelerate onboarding. There is no question that access to the relevant documents, across locations and across clients, is more efficient and faster than "ping pong" emails. The ability to collect documents and data on an organized repository accelerates the processing of such documents and KYC certifications are validated more quickly.

a. POC Deliverables

The deliverables of the POC on Digital Identity Vault for Self-Sovereign Corporate Identity are the following:

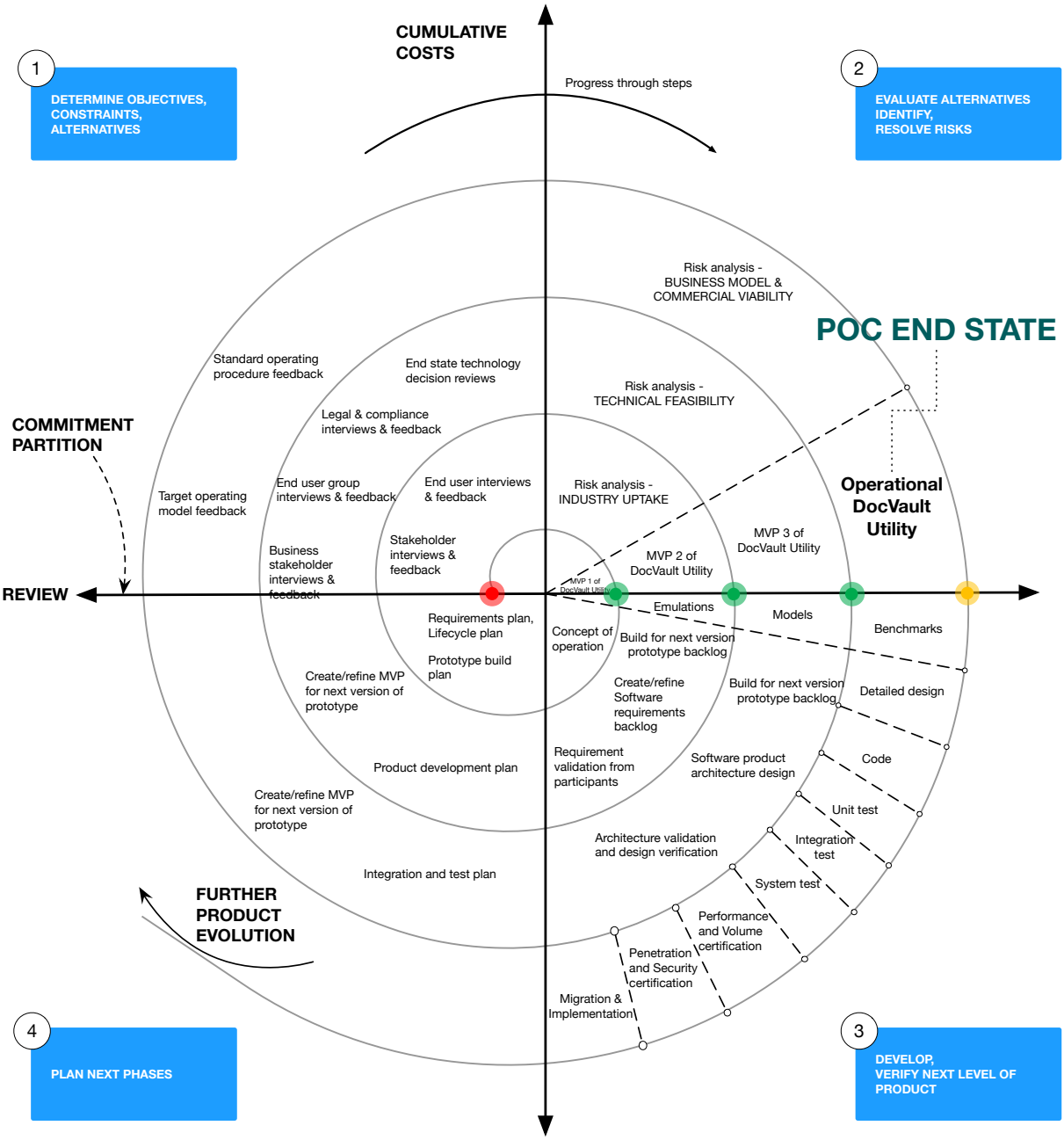
- Build a digital vault that allows clients to deposit their identity documents,
- Build a consent module for clients to present their identity documents to others,
- Design and plan for a DLT / private ledger that allows to move from a centralized state to a decentralized and distributed state.

The term "identity documents" refers to all data or information required to process a KYC, i.e. public and private documents, as well as questionnaires or forms that are part of either onboarding or re-certification processes. For a client to deposit their identity documents, this means the ability to store all these documents.

A "consent module" for clients to present identity documents to others means the ability to share documents, and manage access rights accordingly. In addition, the lack of standardization in KYC processes implies that banks, for example, regularly request additional information to complete an onboarding file or to re-certify a counterparty. Documents needed to comply with these "non-standard" requests are an integral part of the "identity documents" pack of an asset manager, hedge fund, MNC or corporate for the purpose of a KYC process. A "consent module" therefore needs to provide with the ability to (i) share documents while managing access rights accordingly, and (ii) enable a document provider to provide additional documents within the platform, as and when needed, to answer specific requests.

b. Objectives

An operational document vault utility was the POC's first expected outcome. We defined a road map from prototype to an operational platform., which was an iterative risk adjusted project as illustrated by the diagram below.


1
DETERMINE OBJECTIVES, CONSTRAINTS, ALTERNATIVES
CUMULATIVE COSTS
Progress through steps
2
EVALUATE ALTERNATIVES IDENTIFY, RESOLVE RISKS
Risk analysis - BUSINESS MODEL & COMMERCIAL VIABILITY
POC END STATE
Standard operating procedure feedback
End state technology decision reviews
Risk analysis - TECHNICAL FEASIBILITY
COMMITMENT PARTITION
Legal & compliance interviews & feedback
Target operating model feedback
End user group interviews & feedback
End user interviews & feedback
Risk analysis - INDUSTRY UPTAKE
Operational DocVault Utility
Business stakeholder interviews & feedback
Stakeholder interviews & feedback
MVP 3 of DocVault Utility
MVP 2 of DocVault Utility
REVIEW
Emulations
Models
Benchmarks
Requirements plan, Lifecycle plan
Concept of operation
Build for next version prototype backlog
Prototype build plan
Create/refine MVP for next version of prototype
Create/refine Software requirements backlog
Build for next version prototype backlog
Detailed design
Requirement validation from participants
Software product architecture design
Code
Product development plan
Create/refine MVP for next version of prototype
Unit test
Architecture validation and design verification
Integration test
System test
Integration and test plan
FURTHER PRODUCT EVOLUTION
Performance and Volume certification
Penetration and Security certification
Migration & Implementation
4
PLAN NEXT PHASES
3
DEVELOP, VERIFY NEXT LEVEL OF PRODUCT

c. Commercial validation

It was also paramount for us that we build a product with a true commercial application, i.e. that can be marketed to and used by clients as we reach the product end state. This goal cannot be reached without clients' validations. We have therefore interacted regularly with documents providers and documents recipients alike, throughout the duration of the POC.

d. Features

The document repository built on "traditional technology" has been developed with the following features.

Document Exchange

- Document storage
- Upload and download of documents
- Customized document filing through creation of folders and sub-folders
- Document preview
- Ability to set document properties
- Entity Unique ID
- Linkage parent-child between two entities that share a number of KYC documents,

Consent Based Access

- Consent based access rights and management of user's access rights at different levels of granularity:
  - For documents: at folder level, at sub-folder level and at individual document level
  - For users: at entity level, at group or team level and at user level

Audit Trail

- Audit trail on a document, or on a folder, that is exportable
- Audit trail on uploads, downloads or views
- Segregation of audit trails depending on the role and rights of the user(s)

Forms

- Ability to fill a KYC questionnaire or other regulatory forms in the platform
- Ability to share and provide access, in the platform, to a questionnaire or a regulatory form

Expiries Management

- Visualization on expiries calendar and on status of documents
- Documents expiries management functionality

Email summary of all notifications

- Summary of notifications sent by email to users on a daily basis
- Dashboard to manage user's preference

Collaborative tools

- Ability for a recipient to send a document request to a provider
- Ability for a provider to reply to a request, within the repository and without usage of email, and directly share the requested document(s)
- Ability for a recipient to upload their onboarding pack and share forms with providers

e. System Design & Architecture

1. Tech Stack

The document repository is a web-based application with a physical document vault and a relational database management system. The tech stack includes:

- The mySQL database
- The extJS front-end
- SOLR for indexing and search
- The server logic and API
- The physical document vault

2. System security

Two security audits have been conducted during the duration of the POC, focused on three specific stages of evaluation:

a. Architectonic Design Security Evaluation
b. Source Code Evaluation
c. Penetration Testing Evaluation

f. Data Privacy

The document repository has been built with data privacy requirements in mind. It is especially compliant with PDPA and GDPR requirements.

The third deliverable of the POC was to “Design and plan for a DLT / private ledger that allows to move from a centralized stated to a decentralized and distributed state”.

A repository built on a Distributed Ledger, using blockchain technology, is indeed a solution that has potential to address a number of market participants’ requirements with regards to a KYC repository. It would support both future "Self-Sovereign Digital Identify" and current trust based or PKI (Public Key Infrastructure) based identity. It would also ensure increased trust in the operator of this repository by using secure and encrypted DLT (Distributed Ledger Technology) to provide a decentralized and secure shared digital ledger, inclusive of encrypted nodes and storage, secure network service and identity service.

We envisioned that the current repository, which is interfaced via web browser, would interact in the medium term with the DLT based backend. We were also of the opinion that both versions would have to live alongside in parallel for some time. This belief originated mostly from a commercial logic as a number of potential clients, even if interested and attracted by the concept of a DLT and its usage to solve business problems, might not necessarily be able to adopt blockchain technology yet.

To be effective, a DLT solution is to meet the following requirements:

- Facilitate secure document access from providers to recipients
- Distribute the document based on rules / contract between providers and recipient
- Secure and encrypted document / data storage in transit and at rest
- Capability to have self-sovereign digital identity
- Compliance with regulatory requirements (GDPR) and especially with the right to be forgotten - the information contained in a chain being immutable, personal data contributed to the ledger may conflict with data privacy regulations that include a right for individuals to have personal data erased.

a. Benefits of a repository built on DLT

A Distributed Ledger brings several additional benefits compared to a repository built on a traditional technology.

- Networked integrity

Integrity is encoded in every step of the process and is distributed, not vested in any single member. This means that actions (provision of new identity related data or PIA data, request for sharing a document or identity), decisions (to allow access or revoke access) and consequences of decisions are coded in decision rights, in the incentive structure and in operations. As a result, acting without integrity has high deterrent.

- Distributed power

The fact that there is no central authority creates balance of power that affects provision, access or distribution or any other collaboration of PIA data in DLT network.

- Value as Incentive

Participants are rewarded accordingly as more and possibly different types of participants are active in this collaboration of documents (which is the value in the network), based on the various different value adds (e.g. legal verification of identity or document, continuous update of document, aggregation of document et al) that they bring.

- Safety

Safety measures are embedded in the network with no single point of failure. It provides with not only confidentiality but also authenticity and non-repudiation of all activities.

- Rights reserved

Ownership rights are transparent and enforceable on provision of data as well as consumption while keeping it current. Individual freedoms are recognized and respected. All of these are typically codified in mechanism like smart contracts and placed on the DLT network.

- Inclusion

Like any network effect, DLT in Digital document vault / identity management works better when it works for everyone. Placing DLT at heart of this networked system will definitely reduce the barrier to entry, contribute to value and allow to consume the value at lowered transactions costs.

b. Choice of technology for DLT solution design

Several criteria were taken into consideration when choosing technology used to design and build the DLT. It would first need to suit privacy, flexibility, performance, scalability and security requirements. The following requirements were also key with regards to a use-case for KYC documents exchange:

- Participants must be identified / identifiable
- Networks need to be permissioned
- High transaction throughput / performance
- Low latency of transaction validation
- Privacy and confidentiality of transactions and data pertaining to business transactions

We selected well-maintained systems that enjoy growing customer base and community support, as an indicator of guarantee on technology longevity. Open source was also an important factor. Following are the metrics on which various options were evaluated:

- Network,
- Consensus mechanism,
- Smart contracts,
- Language,
- Community support.

Ethereum, Hyperledger, Corda and Quorum were the short-listed candidates. The below table captures the summary of the evaluation:

	Ethereum	Hyperledger	Corda	Quorum
Network	Public and permission-less	All data is invisible to non-authorized members and restricted messaging paths provide privacy for any subset of nodes.	Privacy - Only parties involved in a transaction have access to the details. No unnecessary broadcasting private info on the entire network Assured Identity - Parties will have assurance over the identify of participants in the network.	A fork of Go Ethereum with privacy-enhancing features
Consensus Mechanism	Proof of work based on computationally hard problems.	Restricted to the subset of nodes involved in the transaction, consensus can be implemented or not. When it is, a Practical Byzantine Fault Tolerance algorithm requiring the participation of all nodes is used.	Uses consensus pools that provide consistent, transparent and resilient uniqueness consensus services.	Voting-based consensus reducing network loads and Byzantine Fault Tolerance
Smart Contracts	All platforms support implementation and execution of smart contracts			
Language	Solidity, Serpent	Golang, Java	Kotlin	Solidity
Community Support	Maintained by an active developer community	Hosted by the world leading open source community, backed up by The Linux Foundation	Driven by the R3 consortium	Supported by JP Morgan's active community

After evaluating the pros and cons of the different platforms we chose the **Hyperledger Fabric** open source blockchain technology platform.

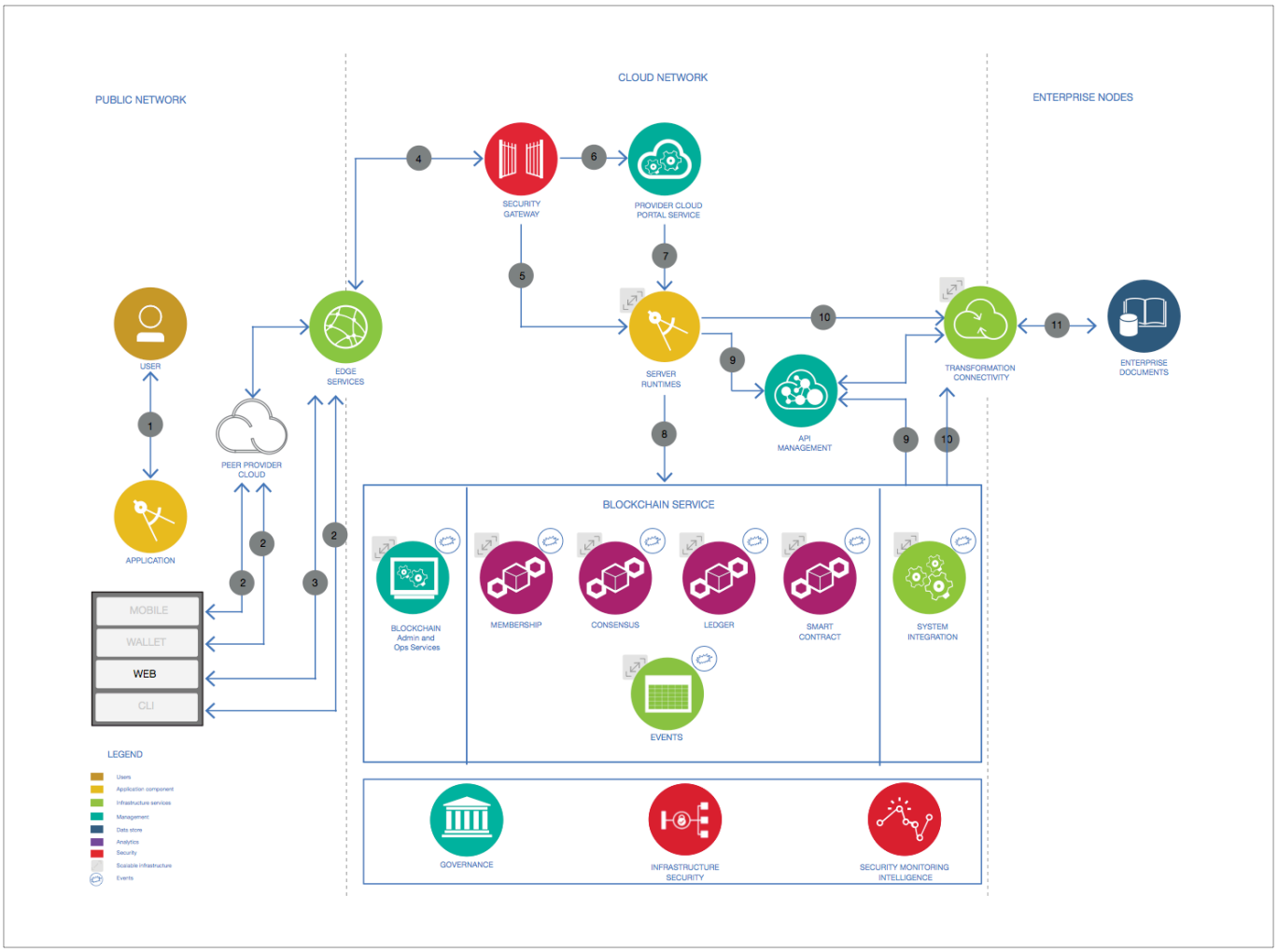
c. Milestones

U-Reg's proof of concept initiative for its document repository using distributed ledger technology consisted for of four key design milestones. They are:

- Experience layer – Screens, Flow and control for persona's identified in journey map
- Distributed ledger and network layer – Design of network and ledger to be used
- Service layer – Design experience layer responsible for business functions and flow as identified by journey map
- Journey map – Identifying key use cases

Key Design and Technology decisions:

The below diagram captures system architecture for a DLT based solution.



Following are the important decisions of solution architecture and design activities:

1. ***Experience Layer***

   The DLT is designed to be a responsive web application, targeted to be used on computers browsers and tablet size devices. This HTML, JavaScript and CSS application uses ReactJS as backbone, JavaScript library to build declarative and component-based application.

   Google's *Material Design System* was chosen as user experience design system.

2. ***Distributed Ledger and Network Layer***

   The following technology stack would be used in this layer:

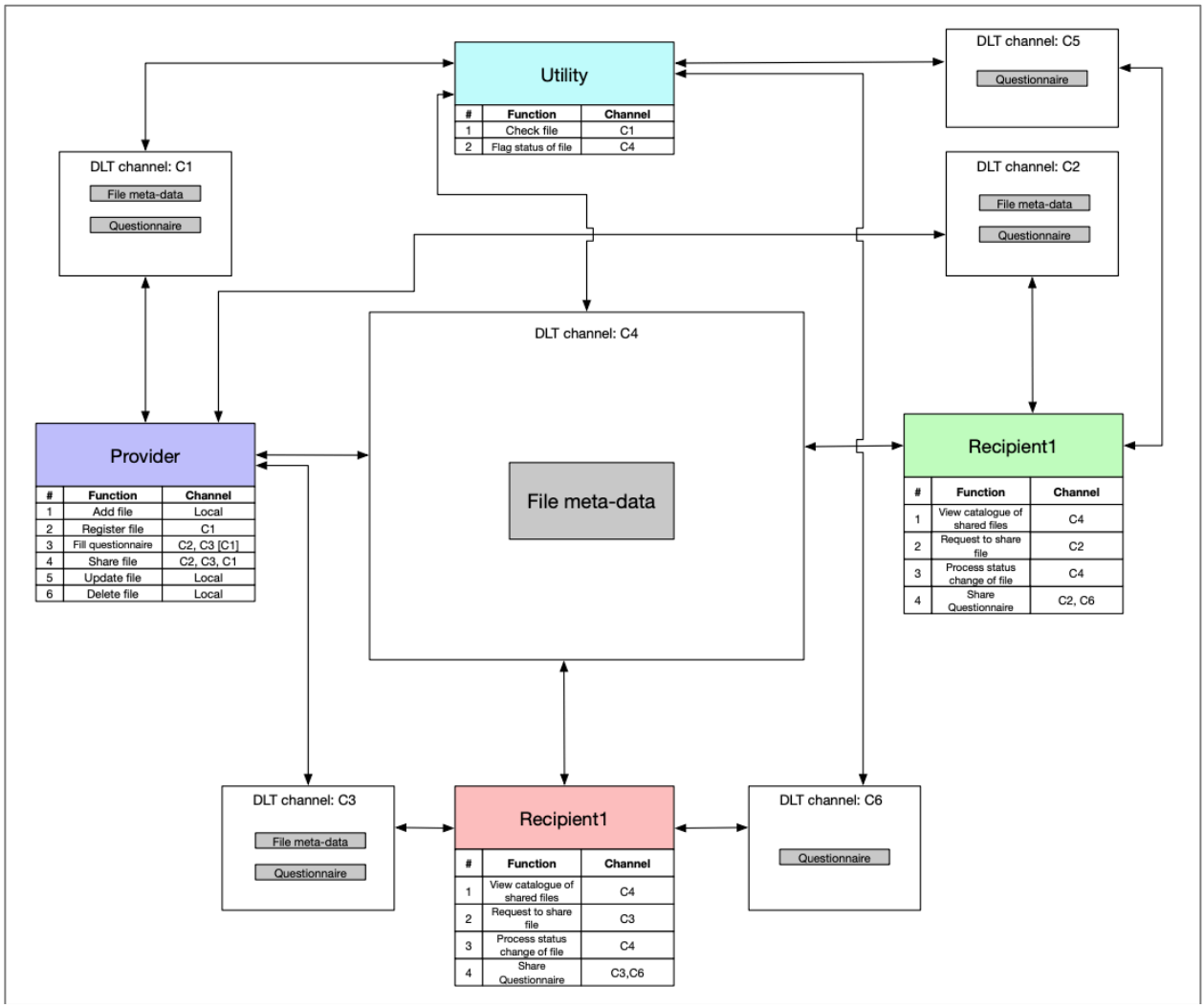
   - Hyperledger fabric (v 2.2.0)
   - Hyperledger Certificate Authority (v1.4.7)
   - Hyperledger Node.js SHIM

3. ***Service layer***

   Node.js was used as backend server environment with polyglot persistence layer comprising of PostgreSQL and Document based database (MongoDB/firebase)

4. ***Journey Map***

   High level use cases were identified as we defined how typical personas will participate in business transactions in target state. We have defined three personas for the initial design - Provider, Recipient and Utility, to which we plan to add other personas, e.g. Registry or Regulator, as illustrated below.



We have then defined several steps where the different personas interact:

- Upload file
- Register a file on the DLT
- Health Check
- View Catalogue
- Form and request file
- Fill form and share file
- Update file
- Delete file

While executing the POC we realized, based on conversation with prospects, that a concept presentation and design artifacts were able to garner inquisitive interest. But it was not decisive enough to assess the adoption potential of the DLT solution in the immediate future.

For this reason, we went well beyond the original proof of concept scope of “design DLT solution” and built a working prototype of multi organization DLT network together with user experience for certain use cases. Following are some screen shots of the working prototype:

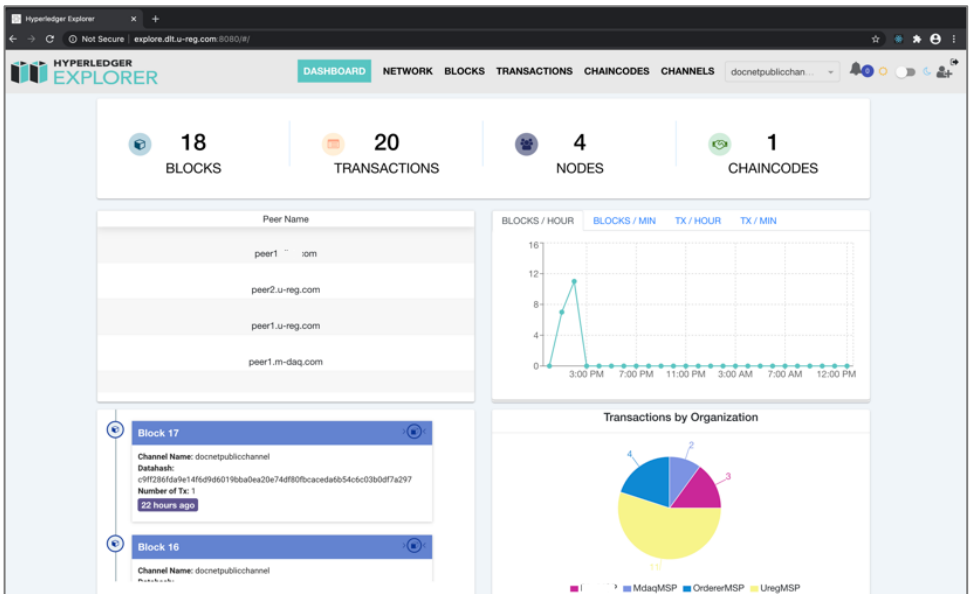


Figure 1 - Multiorg Hyperledger DLT Network

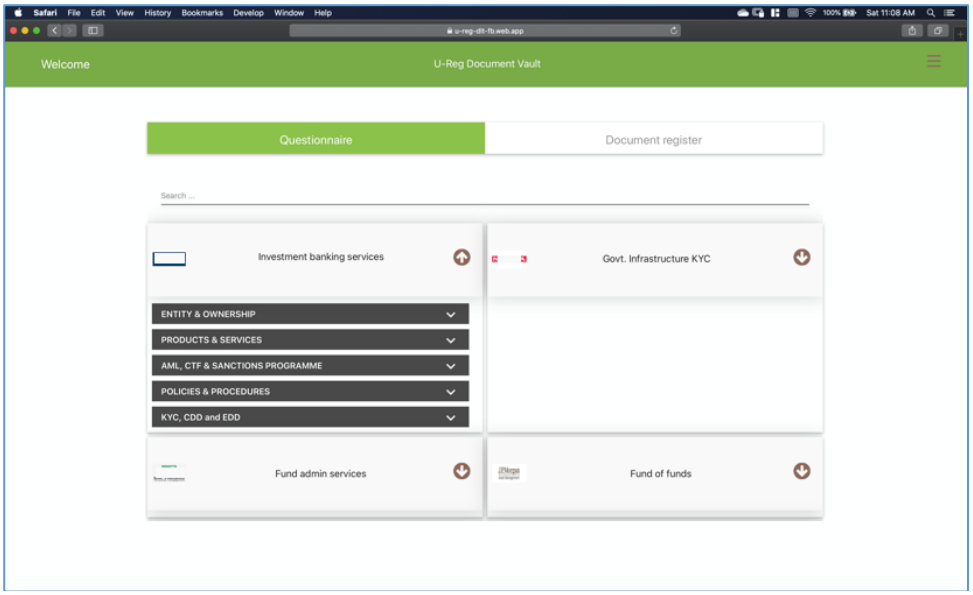


Figure 2 - User Experience Layer

a. Business case

The business case for a repository was established before we started the POC, and it was confirmed during the testing period. Discussions with potential users during the course of the POC and through various meetings where we showcased a prototype, and then a MVP (Minimum Viable Product), confirmed the following:

- There is a need for an efficient solution that reduces the number of interactions during the document exchange process. This is especially true for larger organizations.

- Some large institutions or corporates have DMS (Document Management Systems) that bring a number of efficiencies however these efficiencies are not exportable - their systems are internal and don't communicate with an open ecosystem.

- Furthermore, these solutions are not all dynamic and don't necessarily support a notification system, management of expiries or the ability to do without lengthy email exchanges.

Clients have also suggested that integration of solutions such as screening would increase the attractiveness of the repository solution. It would allow users to process a more significant number of tasks within the same platform.

b. Commercial progress

The repository is live in its traditional form at time of this report, even if developments are underway to bring further enhancements to users. At this point, U-Reg has clients using the repository, as well as institutions who have been onboarded on a trial basis. This was achieved within a relatively short time span and mostly despite Covid-19 constraints, which in our opinion illustrates the needs from end-clients as well as the practicability of a repository solution.

Acquiring a wider network of users is a necessary next step to increase the value of the network. We are in that respect in discussions with large institutions that have expressed interest in the repository but also in other products that U-Reg is developing, mostly the ability to structure data for ongoing management of the regulatory identity of a corporate or of a FI, and resultingly data entry in regulatory forms or questionnaires.

c. Blockchain

Unfortunately, and as discussed below in the "Business and Technical Challenges" section, we do not foresee a widespread development of the Distributed Ledger in the immediate future. This solution

remains attractive in the medium to long term, in principle, for repository solutions and for processes that encompass regular reporting where (i) source of data needs to be firmly established and (ii) there is a need to share such information, on a regular basis, to a network of stakeholders. U-Reg has developed a know-how during this POC that we believe will prove valuable in the future.

This being said, we would like to highlight a possible application of the DLT and a specific opportunity with regards to ESG reporting. U-Reg is currently in discussion with a financial institution that structures and distributes renewable energy assets, managed in a dedicated fund. In this instance, the data used for reporting needs to be certified at origin, and the ability to guarantee the integrity of reporting is an essential feature of the process. A distributed ledger that allows to share assets reporting securely and with integrity on a daily basis, and even possibly in real time with new block created as and when needed, is a solution that appeals to this institution.

a. Testing and Covid-19

The POC started in March 2019 and continued during the Covid-19 global pandemic. This has presented us with several challenges. Financial institutions we had engaged with, and who had been responsive for testing purposes, have faced significant operational constraints. It has been difficult for them to test the system as intensively as they probably would have done in normal conditions. Some that previously expressed interests in U-Reg's prototype had to delay their involvement, in a couple of cases withdrew.

At the same time, we would like to highlight that most have tried as much as possible to dedicate resources for this project. We would like to thank them here for their continuous support, with a special mention for our sponsors who have made sure they remained available through a number of VCs or virtual meetings during what was a challenging operational environment.

b. Network effect

The ability to build a network of users is key for the success of a repository. Feedback has been positive on the capabilities or functionalities of the solution, at the same time the lack of a network effect during the early stages of development can be a deterrent for potential early adopters. We have identified several solutions to remedy to that specific challenge.

c. Adoption of start-up solution

FinTechs, as innovative as they are, are by definition less established than traditional players. Their agility and ability to deliver innovation does not always compensate for the inclination of some clients to favor traditional service providers, seen rightly or wrongly as "safer". There is a need to overcome perceived risks in early adoption, here too we have identified several action items to try to address this point.

d. Market readiness for DLT based Solution

Finally, we would like to highlight some observations on the immediate adoption of a DLT based solution. We noted the following key challenges faced by decision makers within our target customer base:

- Lack of clarity on the terminology and perceived immaturity of the technology
- Insufficient evidence that added technology and operational costs to maintain DLT node(s) will lead to either business gains or increased regulatory compliance
- Perceived risks in early adoption and likely disruption to existing practices
- High costs associated with required FTE with DLT skills set
- Perceived complexity in integrating a DLT solution with legacy systems

We would like to thank the Monetary Authority of Singapore (MAS) for their support. Their commitment towards Singapore-based FinTech companies, their involvement in the FinTech ecosystem and their willingness to empower a POC run by a start-up allowed us to push the boundaries of our innovation capabilities. We would not have been able to go as far as we went without the FSTI POC scheme. We extend special thanks to Lizhi Chen, who has always been available when we would have questions or need information, and whose guidance and advices have proved invaluable.

We would like to also extend our appreciation to Convex Strategies Pte. Ltd. and to M-DAQ CashPort Pte. Ltd, who first accepted to sponsor our application to the FSTI POC and then dedicated time and resources to share their thoughts and advices on the needs and expectations of the industry. They made themselves available as we went through different stages of development despite both firms facing operational challenges related to the Covid-19 pandemic. Here too we wouldn't have made it without the active support and involvement of David Dredge, CEO at Convex Strategies, and Ben Chia, General Counsel and Head of Legal and Compliance at M-DAQ Cashport.

Finally, we take this opportunity to thank the numerous people across various client segments, technology companies or again in the broader financial industry, who provided us with insight on their processes, on their problems and on potential solutions. They have in many occasions given us advices that have proven essential in ensuring that, through the POC, we develop a product that has a real business fit and concrete commercial applications.