



Presentation on cuublemesh to
the Linux Foundation Akraio 5G
Edge Initiative 7/12/2021

Alan Lloyd co founder
cuuble and cuublemesh

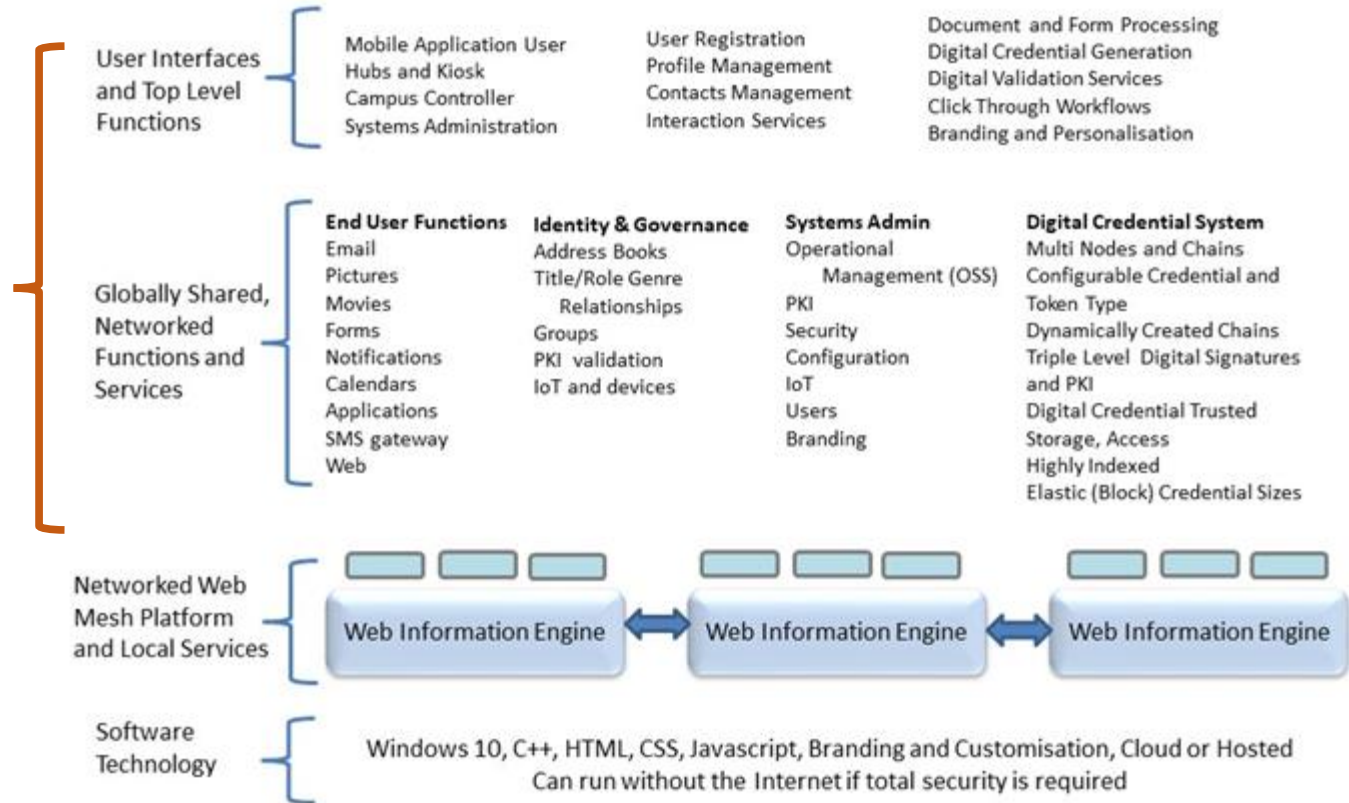
“The gap is between telco networks and cloud interfaces.”

Background and Introduction

- The platform design is based on decades of experience as an architect and software engineer for telco, defence user centric information infrastructure systems taking an identity, governance, security, transformation and operational perspective.
- X.500/509 (directory) and X700 (systems management) . I was on the standards teams. Initiated the Datacraft/Openirectory technology 1988 now owned by CA, it is used by defence, telco, for user based services delivery at scale and PKI. Also developed OSS systems management and service delivery platforms for Telcos/ MSOs.
- Our perspective is that the front end of operational systems are becoming more and more complex, costly and fragmented and present complicated support issues and enable cyber attacks – we must consolidate the functions and build in Zero Trust Architectures.(ZTA)
- We identified the need to have a coherent front end architecture/platform that had integrated web services, IDM/IAM, Content Management, PKI and OSS and with the block chain initiative have legally verifiable “credential” chains.
- But critically, the platform could not be the same as a client-server web server (a portal) or a back office database and transactions. It had to be that of the telco/defence mission distributed infrastructure designs – a meshed nodal system that had its own inter nodal network and signaling capabilities and supported services and interactions.
- And so “The gap is between telco networks and cloud interfaces.” How that gap is filled will need to be a platform system that can work individually, but also work collectively as a real time intercommunicating mesh that handles contextual services but understands users, devices, OSS and network control signals. For the initial design we used the term “social cells”.
- We are now in the position where we are looking for a major company or companies to take cuublemesh into the world or a trade sale of its IP and software.

The cublemesh functions/modules

Many systems world wide will need most of these functions to be coherent from an identity, governance and trust perspective if the ZTA agenda is to be achieved.



Question: Does one design a system starting with its basic processing components or with all the functionality that is fundamental for it to exist in its commercial or social user centric trusted and verifiable operating environment?

A generalised user centric DLT / IoT meshed web platform that provides digital credentials, PKI and operational and service delivery support services.

It contains:

- a unique meshed web services engine,
- a unique user identity and access address book system,
- a unique multi node, multi digital credential chain system,
- a unique multi node PKI and OSS (SDSS) system,
- a unique document / credential e and d signing system

The platform supports applications such as live stock bio security and traceability and digital signature systems.

Address Book: Users, Devices, IoT, Services, Livestock. etc



The unique meshed based address book (IoT) system is interaction-relationship based - role/title/class and genre, it has 3 levels : mesh, node and end users/devices. Entries can be users, devices, 5G equipment, digital credential chains, users, students and live stock (with IoT devices).

OSS Basic Functions



Managing Users, Digital Credentials and PKI - Certificates



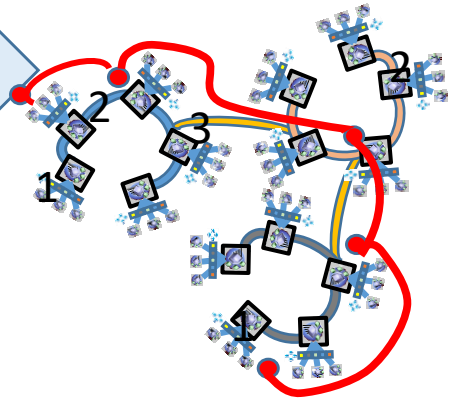
The unique multi node digital credential chains and their users/devices signatures and certificates, etc can be inspected and managed via our SDSS

The problems we address (1): Back Office->Portal->Client Server

Problem 1: With the exception of Telco and Defence, **most systems get designed from a process-transaction-database perspective which usually results in a silo process.** This compromises trust and usability, personalization, the identity, systems management, the operationalization, networking and front end security which is the hardest part.

And: **client-server – means one end of the system is in charge.**

- The cuublemesh web engine is unique – evolved from the user centric wwiteware service delivery platform (SDP) evolved from directory enabled SDPs, evolved from industry grade directory systems – identity and PKI – systems transformation and convergence. See...
- <http://cuublecloud.com/papers/wwDirSDPEvolve.pdf>
- <http://cuublecloud.com/papers/SDPSandPBAC.pdf>
- <http://cuublecloud.com/papers/DeliveringUnifiedServices.pdf>
- Inter nodal interface is bi-directional client server.
- The interface - OSS, chain search, address book functions, PKI functions, etc
- The interface has inbuilt proprietary security / encryption methods.
- Nodes, users, devices, credential chains have IoT addressability.
- Nodes use several groups of micro services and internode micro services.
- Nodes discover other nodes and get their status and configuration.
- Nodes support multiple credential chains.
- Nodes support both local and distributed applications.

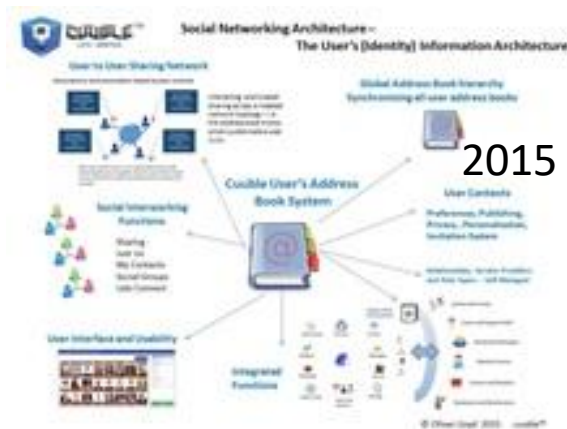
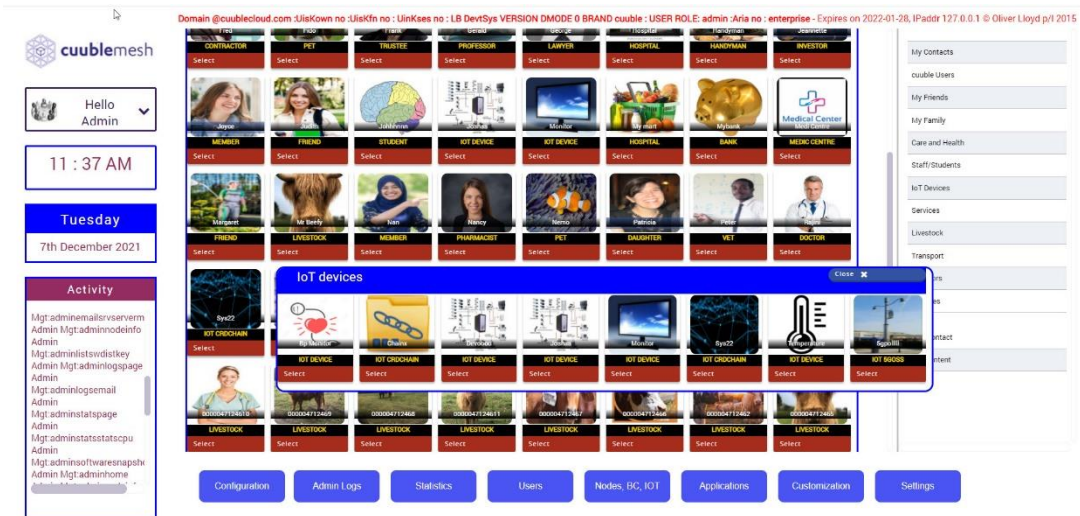


E.g. Supply Chain,
Legal, Health Care,
Bio Security, 5G
content

It far easier and quicker to design systems that can be demonstrated - with a web engine and onboard support functions than starting a design with a data base model.

Problem 2: Identity and governance designs – these underpin all aspects of security and interworking – Usually seen as users or devices logging on. These are identified in the context of the hierarchical organization in a singular manner. However users and devices interact across organisations. But critically we identify, relate to and trust other entities via their name, title, role, image and genre of the item concerned and we want to configure or dynamically change that ‘interaction identity’ context for ourselves.

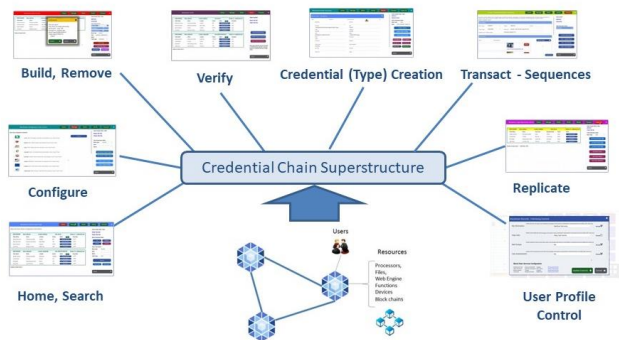
- Our approach is to design systems from an identity, governance and information services delivery and usability perspective and then we engineer the data level functionality that supports that.
- Beyond the meshed web engine, the foundational design element of cuuble/cuublemesh is its address book (its distributed directory) – the address space is flat and used at three levels – the system-mesh, a node, a user/device/service/chain/livestock or 5G entity level - all IoT addressable.
- It has a software configurable role/title class and genre scheme and supports groups and private entries. It’s the way people find things that is critical, sometimes not by name but by function, role or genre.. And being web – its click through.
- Because there are many types of address book entries, we accommodate the variant attribute sets. A user is different from a device, a student, livestock, a service, a credential chain or a 5G device or pole. All have variant attributes.

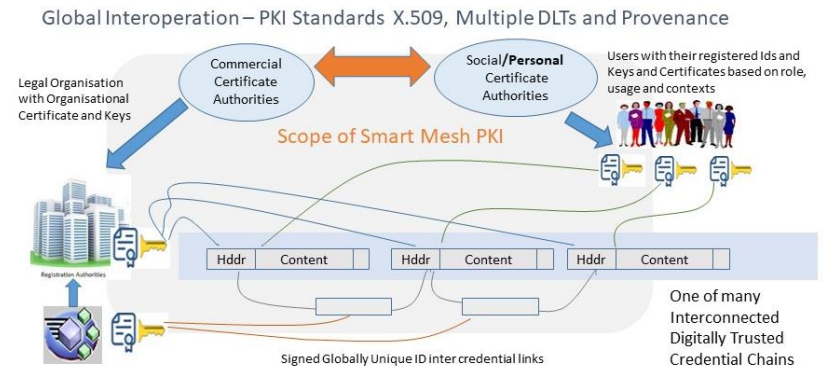
The screenshot shows the cuublemesh user interface. At the top, it displays the user's name 'Hello Admin' and the time '11:37 AM' on 'Tuesday, 7th December 2021'. Below this is an 'Activity' feed listing administrative actions such as 'Mgt: adminmailto:vservm Admin Mgt: adminnodeinfo Admin'. The main content area is a grid of 'IoT devices' categorized by role, including 'CONTRACTOR', 'PET', 'TRUSTEE', 'PROFESSOR', 'LAWYER', 'HOSPITAL', 'HANDYMAN', 'INVESTOR', 'MEMBER', 'FRIEND', 'STUDENT', 'IoT DEVICE', 'IoT DEVICE', 'HOSPITAL', 'BANK', 'MEDIC CENTRE', 'FRIEND', 'MEMBER', 'MEMBER', 'PHARMACIST', 'PET', 'DARTER', 'VET', and 'DOCTOR'. A 'Livestock' section is also visible. The interface includes navigation buttons for 'Configuration', 'Admin Logs', 'Statistics', 'Users', 'Nodes, BC, IoT', 'Applications', 'Customization', and 'Settings'. A status bar at the top right shows system information: 'Domain @cuublecloud.com :UserKown no :UserKfn no :LinkKses no :LB DevSys VERSION DMODE 0 BRAND cuuble : USER ROLE: admin :Aria no : enterprise - Expires on 2022-01-28, IPAddr 127.0.0.1 © Oliver Lloyd p4/ 2015'.

Problem 3: Block Chain from an user centric information systems perspective is designed as a database that is replicated – a silo. The BC block linkage cryptography methods only deal with data integrity so from a global identity, PKI legally verifiable trust perspective – e.g. HTTPS/509, BC is very weak. Small block sizes constrain applications leading to overspill of system components, complications and less trust. There are also over 3600 BC patents owned by many companies, meaning BC software and services supply could face infringement notices.

- ⦿ We have designed an IoT addressable multi node, multi chain system. It has extensive horizontal and vertical indexing.
- ⦿ It uses ISO/ITU/Defence standards X.509 attribute certificates (Defence approach) as its blocks – they are all digitally signed, providing credentials and legal proof of provenance.
- ⦿ It has configurable credential types and token types – the credential being the content, the token used for its value.
- ⦿ It has elastic block sizes, can hold images, movies and multiple content types in the same credential. Tested to 230MB
- ⦿ It has 3 levels of digital signatures – that of the legally verified organization, one of the system’s name that controls the chain and the other of the author of the content – legally verifiable trusted and globally administered identity regimes and provenance.
- ⦿ It supports the dynamic creation of system level or personal level credential chains.
- ⦿ It has a built in smart mesh PKI system combined with its OSS to support the system wide credential chains
- ⦿ It has a chain/block devops style systems management and viewer functions – which can even play the movies held in a credential – See our multi node multi chain search performance figures are on our cublemesh web site,
- ⦿ Is now integrated with cublemesh document and image e-signing and digital signing work flows.



The cublemesh multi node, multi chain, credential chain system has been designed from a dev ops – systems management perspective – verification tools included.



Chain and Credential Links Management

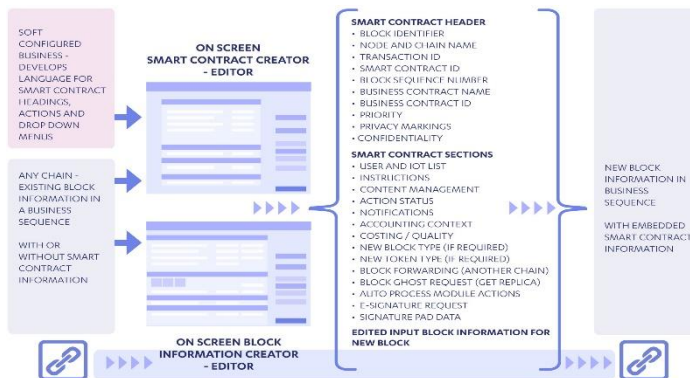
Problem 4: Block Chain smart contracts - a software development agenda trying to relate to legal systems and lawyers.

The existing and traditional data oriented DLT strategy is for a single chain replicating the data to another system.

The ‘replicate every data item to everywhere’ approach can be problematic for larger systems re reliability, data management, scale, inflexibility, interoperability, operational error conditions and TCO. Also the smart contracts are written by software engineers but now with Smart Legal Contracts they need to be legally described and hopefully digitally signed.

Collectively all of the above issues are well beyond normal office automation users.

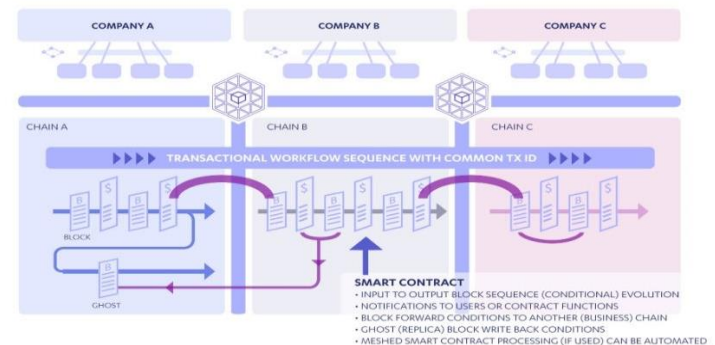
- The cuublemesh smart contracts architecture allows for a multi node, multi block chain system to manage multi block transactions and for the block and its smart contract to be stored and replicated to other block chains under a business-operational DLT strategy. This functionality allows for business relationships to determine how the DLT is collectively applied.
- The cuublemesh system applies flexible business – user level smart contracts for the business contract itself and the controls to determine the system’s DLT functionality on a per credential chain transaction use-case basis.
- The smart contract architecture applies our peer-to-peer mesh web services engine to search for and to write to the block chains across the mesh.
- The business level user controls are via a block creator-editor function, smart contract creator-editor function and a business-operations user configured smart contract language module.
- The execution of the smart contract at each stage of the transaction’s block creation sequence can be via human user methods, automated methods or a combination of both.



(Unique) User Configured Multi Chain

solving blockchain scaling with smart contracts

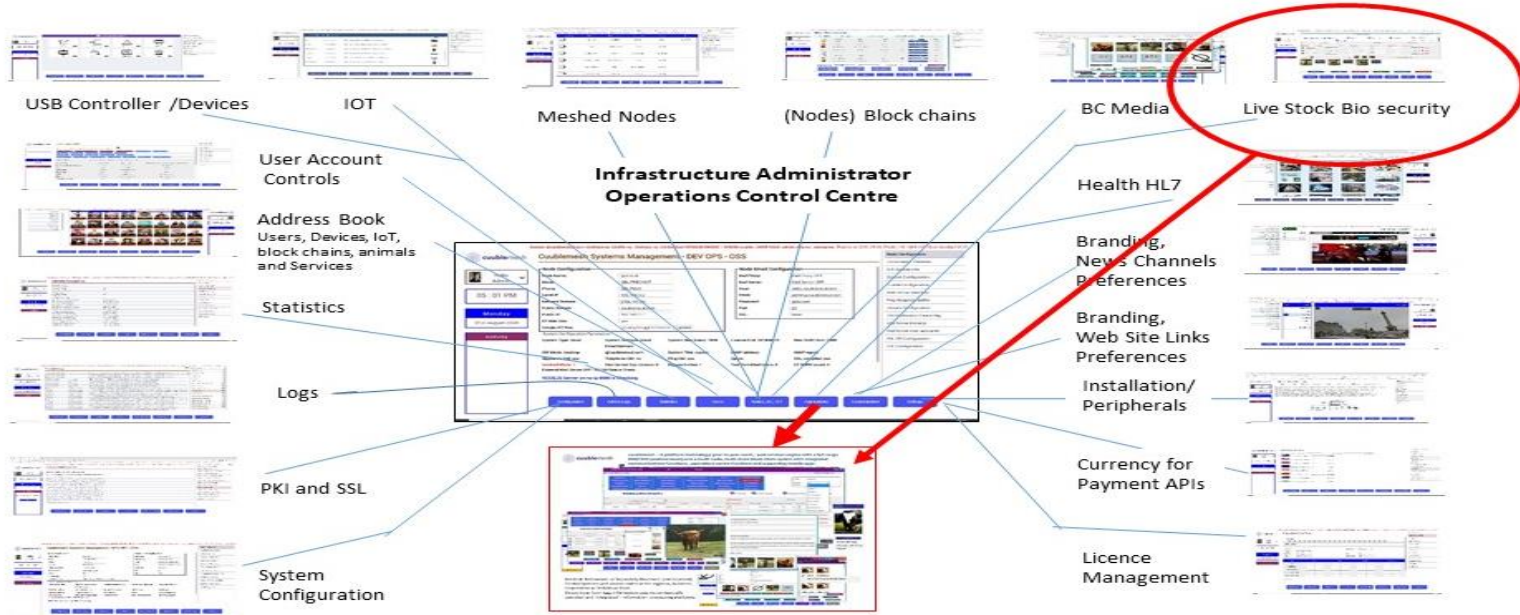
For supply chain, legal, health care and other transaction sequences



Problem 5: Commercial process centric systems tend to have a tactical approach to the systems management and security needs. This means many systems do end up with application silos and a plethora of fragments of supporting functions. While small, such systems are manageable, when large they become impossible to address how to evolve or enhance them. Coherent OSS designs as per ISO/ITU standards X.700 and the TMN M. series standards – like X.500 are information systems level engineering methodologies that relate well to software architecture and engineering. For multi node systems, this engineering approach is essential.

- The platform functions that fit in the gap between the telco and the cloud are dealing with just about everything. OSS is complicated and overarching. Everything from web logs, SSL to managing livestock and food supply, smart city events and cyber attacks.
- Our architecture retains the mindset that every item in the system is a managed object – So one is building a seriously big and distributed (inter-nodal) directory of legally/IoT identified managed objects – see X.500 and X.700.

The current scope of the systems management functions – using the cuublemesh ADMIN interface,



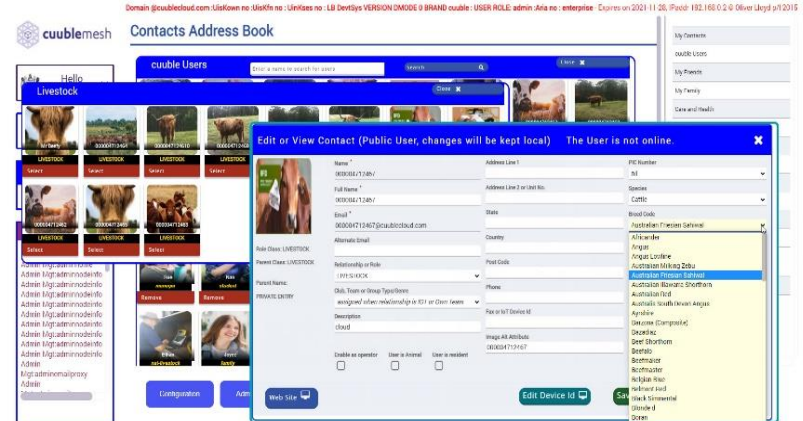
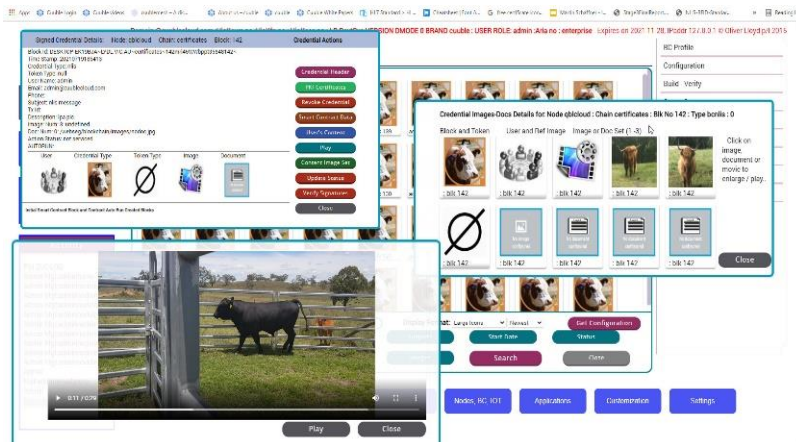
Problem 6: Organisations deal with forms and documents of various ages , designs and standards. Digitisation and process simplification will reduce operating costs and the use of images, videos , voice recordings , e-signing and digital signing and credentialising present a significant task. It’s a task we always do with service delivery systems and it’s a task we do quickly on the cuublemesh platform – because it is a web engine.

When dealing with infrastructure, multi party online legacy systems,data quality, usability, accuracy, provenance and extensibility issues are key . We worked on all of the National Livestock Information Standards (NLIS), the Meat and Livestock Association (MLA) and Livestock Producers Association (LPA) forms and reworked them for end user generation and trusted reporting via digitally signed credentials. The steps...

1. Review Data, Forms, Reports, Governance Information Standards, Normalisation, Provenance and Operational Usability
2. Creation of Web Forms: Services Context, Fields, Catalogues, Content Inclusion, Signatures, Work Flow, Recipients and Trusted Features
3. Credentialising: Digitally Signed Storage, Legal Verification, Searching, Management, Identity and Governance
4. Usability: Users, Devices, Content Media, Live stock, Services, Organisations, Systems Nodes and Chains

The credential with form data, images and video

The address book with livestock entries and MLA info

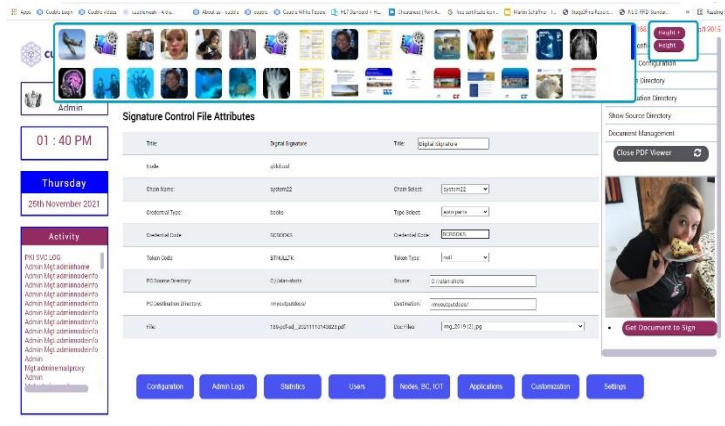


Problem 7: The digital content of organisations represent valuable assets which can be identified, catalogued, searched, and traded and digital proof of provenance is needed. ie NFTs . But block chains with small block sizes have to outboard the content and the BC block signing algorithm doesn't seem to use legally recognized identity based PKI systems

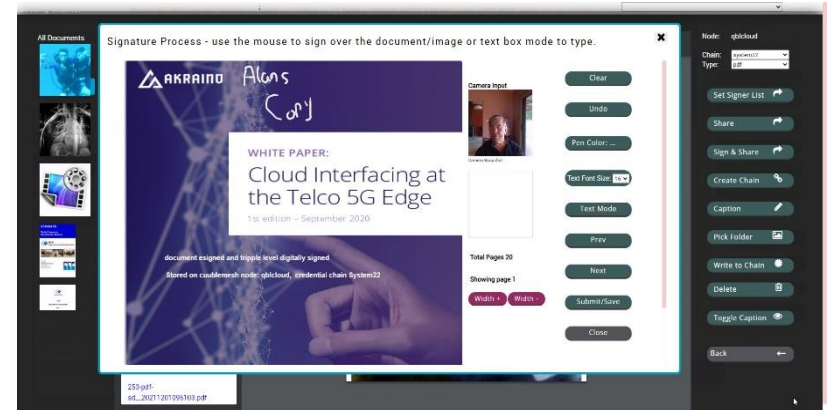
Our approach to legally verified digital provenance:

- ZTA and multi signed documents, forms, images, movies, etc - scratch over them , sign them, create overlaid text boxes, select pen colour, font size and snap shot the e-signing. Then store it as a searchable , digital credential type and on the chain of ones choosing. ie Trusted NFTs
- We can set the signature list from our address book identity system, sign and share, create a new chain dynamically and signal others in the supply chain re the content process needs.
- If we couple our content management system to our smart contract, multi chain, auto schedule functions, we arrive at say 5G - Supply / Smart city as a service, using 5G poles, location specific services activation.
- Smart cities for example need contextual services environments: processions, sports events, climate change issues and emergencies.. all will be based on ZTA verified trusted content and systems management and contextual credential chains.

The OSS set up



A user – markup and signing



In the presentation I have presented what we see as seven critical systems engineering issues that take us from the back office database era into the trusted online infrastructure era, based on telco and defence, based systems engineering, transforming legacy systems and avoiding silos.

We have addressed them all with a new breed of system. We fill the gap between the telco and the cloud from a user and trusted online and dynamically configurable infrastructure perspective.

Key Features

- A unique networked web / IoT services engine with its own identity, governance, PKI, OSS and end user and application functions.
- A 'Front End' Internet or Intranet platform designed and built as per Telco or Defence Mission Systems where trust and systems management is key. **Can run with or without the Internet.**
- Designed for multi party digital infrastructures , supply chains, where user, devices and services interact in a trusted and self managed way and where legally verified identity and data provenance is fundamental.
- Being a platform it can be used as a System's transformation tool or for functional developments – where the software can be applied to the legacy environment.
- Uses a unique multi node, multi chain, multi block type, trusted / PKI digital credential system.
- Can be branded, easily integrated and fully supports the Zero Trust Architecture agenda.

Totals about 18000 files- we have a file scan – code listing utility.

HTML, JS, CSS appx (includes about 100 open source JS)	5000 files
Images - configurable appx	6000 files
C++ The meshed web engine appx	2500 files.
Executable Modules appx	250 files
Others inc Traces-Configuration appx	3000 files

Does not include User Environment Data
Does not include Apps software modules

- ☸ IDE is Microsoft Studio, Chrome, extensive JS, JQuery - dynamic web pages.
- ☸ It can support the hmail opensource email server /sql database
- ☸ Cuublemesh time has come.
It is complex by nature but integrated and easily integrated and branded with existing front end web services systems.
- ☸ From a systems engineering perspective a great saying is:
Existence proof is everything – we present cuublemesh with its screen shots.
but being web screens they can be customized.
- ☸ **All the IP except for the open source modules is owned by oliverlloyd.pl**
- ☸ **We are open to a trade sale or a global distribution arrangement that addresses the global deployment of the platform and its social-business utility.**

Web site is cuublemesh.com and cuuble.com

Linked In – Background design – Defence Mission Systems:

https://www.linkedin.com/posts/alan-lloyd-82a38a_identity-and-governance-evolution-of-cuublemesh-activity-6849586665812570112-QrS-

Linked In – Systems Architecture:

https://www.linkedin.com/posts/alan-lloyd-82a38a_systems-architecture-from-the-user-experience-activity-6841216582128164864-2lDf

Linked In – Smart PKI and OSS operational platform designs

https://www.linkedin.com/posts/alan-lloyd-82a38a_cuublemeshsmart-mesh-pki-and-oss-platform-activity-6818772434586624000-f-5m

Linked In – Taking the Livestock Legacy Systems onto the platform

https://www.linkedin.com/posts/alan-lloyd-82a38a_cuuble-mesh-re-livestock-and-food-supply-activity-6825729962604138496-49bg

I would like to thank Ike Allison for the excellent 5G information and support and the discussions we have had over the last few years. Ike is highly informed, a leader and dedicated to the global 5G outcomes being the best we can achieve.

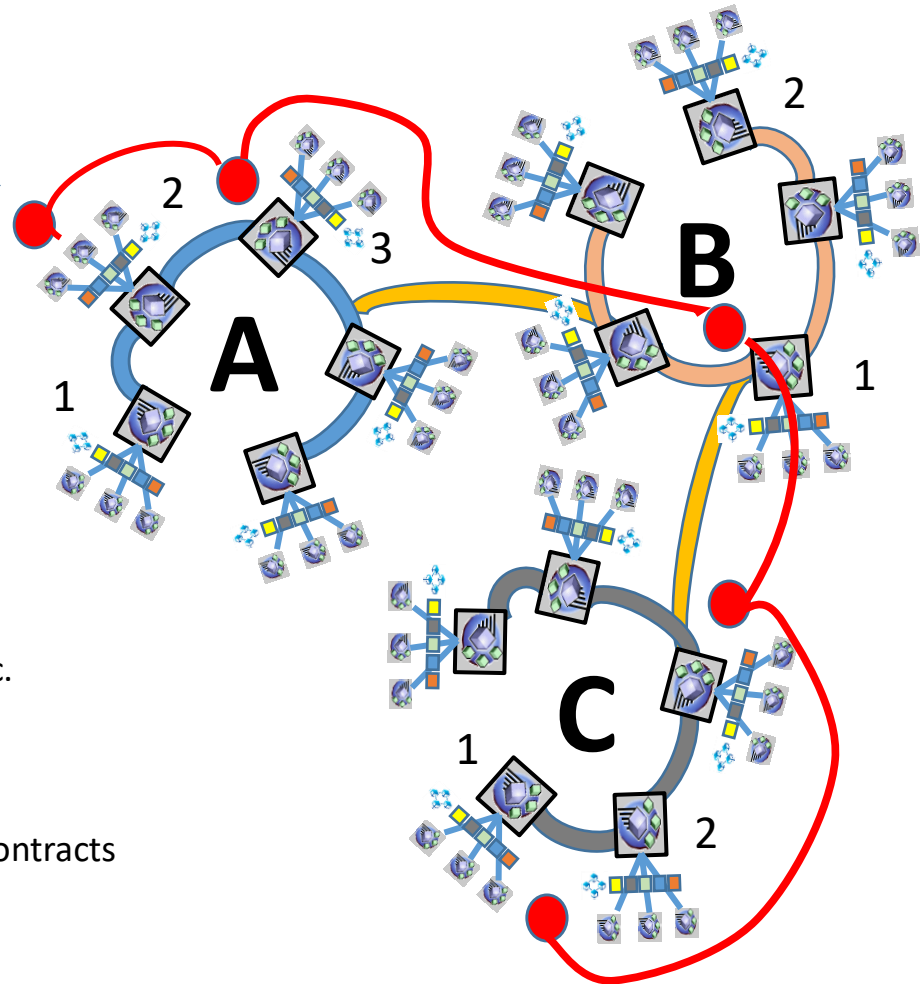
From my journey the world is moving to a new regime on online infrastructure systems. Trusted, managed at many levels, situational, mission based almost, certainly interaction based and contextual, experience based. But must relate to and be engineered to the global identity systems we have – our white pages, and be accessible.. socially minded nodal cells maybe.

Technical data mechanisms should not lead this agenda but be used as appropriate. And technical mechanisms can never change the white pages (x.500) global identity contexts and infrastructures that we work with and use daily – and thus its information systems engineering methodologies.

Attached some useful slides on supply chain mesh systems and the uses of the existing global PKI /x.509 systems.

Thank you for your time and attention.. All appreciated.

E.g. Supply Chain, Legal, Health Care, Bio Security, 5G content
'Transaction Sequences'



The need for:

- Decentralised Meshed Environment
- Multiple Nodes
- Addressable Nodes, Chains, IoT devices
- Multi Credential/Block Types
- Multi Token Types
- Cross Mesh Search on Transaction Ids etc.
- New/Next Block Routing
- Credential Activity Status Services
- Transaction Sequence Managed Content
- Transaction Sequence Managed Smart Contracts

In this scenario we are dealing with digital credentials in the context they are created – but these can be copied back to a central system as required.

We are also dealing with the global scope of PKI systems, legally verifiable trusted identity and domain names, credentials, provenance.. It is critical that the new age decentralised OSS and SDSS adopts the Zero Trust Architecture Agenda and can service the new digital entities e.g. smart contracts, livestock management, smart cities with 5G.

PKI – Identity, Governed, Web-IoT Cryptographic Key Managed View of Digital Signatures and Multi Chain Systems - Credentials

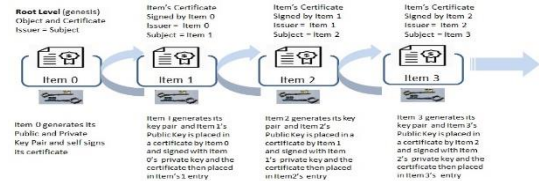
X.509 (1993) – Section 7: “This common point of trust (the root level) shall be linked to each user (item) by an unbroken chain of trusted points”



X.500 Directory (Identity) Hierarchy

Figure 4 – CA Hierarchy – A hypothetical example

X.500/9 Directory (Trust) Hierarchy



CA Signs Certificate Chains



Web HTTP SSL/TLS Traffic



SMIME Messaging



Military Messaging Attr Certs



OCSF Inter agency - companies



Software Downloads



Organisational Certificates



Signed Digital Tokens / Credentials



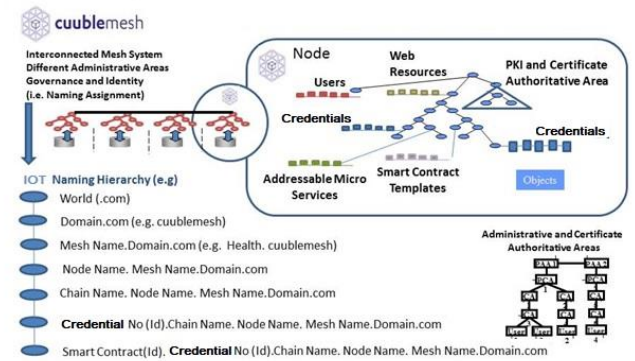
Signed Digital Assets / Content



Signed CBDC and Certified Banks



Signed Smart and Legal Contracts



Noting it is likely that Tokens, Assets, CBDC, Contracts and Legal Documents may require several signatures thus the top level signed chained credential content can be a sequence of digitally signed credentials – a composite digital signed certificate chain.