TAG Distributed Ledger Technology (DLT) Industry Consortium Network

Industry Consultation Document

September 2020

Table of Contents

1. Overview

Online Digital advertising has been a fast growth market since its inception over 25 years ago and transparency in digital advertising's supply chain is critical to its sustainable future. Much has already been done to achieve that, not least through TAG brand safety and fraud standards, but there is still much to be done - The recent PwC study commissioned by ISBA and AOP highlighted the complexity of the programmatic supply chain and the need for industry consistency around data sharing and formatting, and we are all aware of the growing pressure from regulators to prove the compliance and accountability of digital advertising.

TAG's remit is to address the trust and transparency challenges the industry is facing. This includes assessing how new technologies can help the industry continue to self-regulate through standards, certifications and best practices and to ensure they are enforced at all times, consistently and by all industry participants across the supply chain.

At TAG, we believe that many of our industry's trust and transparency challenges can be resolved by setting up an industrywide collaborative environment that guarantees the proper implementation of common rules among participants using appropriate technology. To this end, TAG has been working for the past year on evaluating the benefits of an Industry Consortium Network using Distributed Ledger Technology (DLT) as an "always on" solution.

Together with the JICWEBS board - formed by ISBA, IPA, IAB UK and AOP - we identified in 2018 that Distributed Ledger Technology (DLT, also known as Blockchain) was a promising solution. DLT could raise standards and address the trust problem, while driving a range of additional industry benefits.

a. The TAG/JICWEBS DLT pilot

In March 2019, JICWEBS and its board decided to run an extensive, multi-faceted pilot project to put DLT to the test. It set out to evaluate: if (a) DLT is suited for digital advertising, (b) if JICWEBS as a cross-industry trade body is the right home for it, and (c) what DLT technology platform is to be implemented should the board decide to launch the network.

The pilot has been running since July 2019 with major industry brands, including **Nestlé, McDonalds, Virgin, O2/Telefonica, Unilever, Johnson & Johnson**; larger agency trading groups, including **WPP, Publicis, Omnicom, Havas, IPG**; and a number of technology vendors and publishers as part of their supply chains. The Pilot integrated 20 data feeds, analysed 112 million impressions amounting to £1.4M of programmatic ad spend across 127 campaign placements.

Besides the involvement of its own team, JICWEBS created a DLT Evaluation Committee formed of 20 industry and blockchain experts, together with representatives of each of the trade bodies (1). The Committee reviewed the pilot as it progressed, conducted an RFI process to evaluate the offering of different technology providers and made a recommendation to the JICWEBS Board.

The results of the pilot and the evaluation conducted by the DLT Evaluation Committee, led the JICWEBS Board, to come to conclusions on the following questions:

a. **Is DLT suited for digital advertising?**

   The Pilot has provided evidence that DLT is particularly well suited to address the trust, transparency and efficiency problems the industry is facing. Immutable impression audit trails and the use of smart contracts enhance accountability and compliance while driving significant incremental business value and operational efficiencies for participants.

b. **Is TAG/JICWEBS the right home for an industry wide DLT initiative?**

   The initiative is directly in line with the mission given to TAG/JICWEBS by UK's major trade bodies to "oversee the independent development of Good Practice and Standards for digital ad trading."

c. **What are the requirements of a DLT industry wide technology platform?**

   The requirements have been defined and a number of technology providers have been evaluated.

(1) The DLT Evaluation Committee was formed of representatives from: IBA, IPA, AOP, IAB UK, IAB Tech Lab, ABC, GroupM, Mediacom, Publicis Media, Seven Stars, Omnicom, eBay, Accenture, PwC, Wirehive, LDTRT, and some independent blockchain and industry experts.

b. Open industry consultation

The purpose of the consultation is to share the details of the initiative and give all industry participants the opportunity to provide their input. This will help us to better define priorities.

We are asking for comments to the Consultation Document so we can understand where you think DLT could add value, what concerns you have, and what we need to do to make this work for you. A large part of the success of this initiative is wide industry adoption, including by the larger industry players. It could go well beyond the UK borders.

This consultation document is written to provide a clear and comprehensive account of the DLT network proposal for a general industry audience. It sets out:

- Why we think a network using a DLT platform is right for the industry
- What benefits members can get from the network
- What a DLT industry consortium network will look like
- How DLT network members will use the network
- What it will take to participate
- The timeline and next steps for launch

We are looking forward to getting your comments on each section of the document. You are strongly encouraged to provide comments even if they are brief, or only to indicate your organisation's overall support.

As part of this, we would be interested to know what other related actions, measures, initiatives we could undertake that would help ensure online advertising can win trust while continuing to grow and be innovative. We would like to know what further role you expect TAG to play in regard to its mission to drive trust and transparency.

The TAG Townhall took place on Thursday **1st October 2020** presented an overview of the pilot results and the details of the consultation process. Following this event, ISBA, IPA, IAB UK and AOP will be inviting their members to join webinars which will present more information and provide an opportunity to ask questions. For those wanting to understand more detailed technical specifics of the network, a Technology Document is also available. This document provides a more in-depth look at the DLT platform and infrastructure and will be made available on request to interested parties under NDA.

The comments we receive will be reviewed by a Steering Committee formed by TAG, the UK trade associations and any applicable experts after which the Steering Committee will provide a set of recommendations. TAG will simultaneously lead efforts to structure a consortium for the post-pilot phase and announce a decision about its role in that effort during Q4 2020.

Some supporting documents and webinars providing background information about the initiative can be accessed below. These documents are not part of the consultation and are only intended to provide background information. You will also find documents referenced in this Consultation Document as well as a list of documents that provide some further background information under Section 11.

- TAG DLT Pilot Report Executive Summary

- TAG DLT Pilot Report

- Technology Document - This document requires to sign an NDA. Please make your request to consultation@tagtoday.net and you will get contacted.

- London Tech Week - Where Advertising meets Technology
  - CreaTech webinar - Sep 7, 2020 (min 45:20)
  - Jules Kendrick, MD UK & Europe, TAG
  - Nigel Vaz, Global CEO, Publicis Sapient & IPA President
  - Tim Brown, CEO, Fiducia

- TAG DLT Network webinars:
  - Webinar 1 - What is the TAG DLT Network initiative all about?
    Jules Kendrick, MD UK & Europe, TAG (min 09:51)
  - Webinar 2 - Can DLT solve the industry trust problem?
    Gavin Stirrat, Industry Expert & Fiducia Consultant (min 16:31)
  - Webinar 3 - What radical changes is DLT driving across industries?
    Richard Brown, Chief Technology Officer, R3 / Corda (min 17:58)
  - Webinar 4 - How does a DLT platform work?
    Igor Alferov, Chief Technology Officer, Fiducia (min 17:30)
  - Webinar 5 - Why should I participate to the DLT Network?
    Phill Hayman, Customer Success Director, Fiducia (min 14:03)

c. How to respond

We welcome written submissions by email to consultation@tagtoday.net in a document format like PDF or Microsoft Word.

The deadline for providing comments is midnight on Thursday **5th November 2020**.

In your response, please clarify:

- If you are responding on behalf of an organisation or in a personal capacity;
- Which sections of the document you are referring to. There is no need to comment on all the sections of the document if they are not directly relevant to you;
- Whether you are willing to be contacted (in which case, please provide contact details);

- Whether you want your comments, or part of your comments, to remain confidential for commercial or other reasons; and

- If you want to engage in person, please specify this. We will try our best, resource-allowing, to find opportunities to do this.

d. Further information

Information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the General Data Protection Regulations (GDPR), and the Environmental Information Regulations 2004.

If you want the information that you provide to be treated as confidential, it would be helpful if you could explain to us why you regard the information you have provided as confidential.

If we receive a request for disclosure of the information, we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding.

We will process your personal data in accordance with the Data Protection Act 2018.

2. The trust problem facing digital advertising

We are all aware that the digital advertising industry faces multiple trust and accountability challenges. There's a lack of trust between industry participants in the supply chain, amongst the consumers that we serve and from inside government.

The recently published ISBA/PwC report into the programmatic supply chain and its headline catching "15% unknown spend delta" may have re-ignited passionate debate about this problem. But it is only the latest analysis to make this point: that the vast complexity of our ingenious programmatic supply chain is still difficult to audit and not very transparent for buyers or sellers. In 2014, the World Federation of Advertisers found much the same challenge in their analysis of the spend 'waterfall'. And in 2017 the Association of National Advertiser's "Programmatic: Seeing Through the Financial Fog" painted a similar picture: simply determining how all impressions are delivered is very challenging. Given what seems to be, at best slow progress, it is no wonder that advertisers have been saying for years that they perceive the supply chain as "murky at best, fraudulent at worst". After all, we have not even been able to make asking *questions about* our supply chain as easy as they should be, let alone actually answer them. And in such an environment, it is unsurprising that trust is lacking.

a. Why it is hard to know what is going on?

This is the most important question of all. Fortunately, the recent ISBA/PwC study provides a potential answer. Quite apart from specific findings about an 'unknown spend delta' or its possible causes, the most important finding was probably about the report itself: how hard assembling the actual data was. ***Only 12% of the 267 million impressions in the study could be matched across the supply chain.*** It took many months simply to assemble the impression records required and much of the data had to be discarded due to low quality. That's a major problem because if you can't even match data sources between supply chain participants reliably, you can't reliably begin to really understand it. Being able to match impressions *should* be the rule, not the exception: but that's not where we are today.

Is this so surprising? Probably not. The innovations of online advertising create a vast amount of data which is spread out across multiple systems, with many different legal arrangements to access. This is true both inside and outside walled gardens. Organisations can freely and quickly participate in RTB auctions directly via APIs or through different UIs that sometimes have a low bar for vetting or identify verification - making even knowing the real identity of other participants a challenge. Even where data is officially available, the friction of working across disparate data sources in different organisations, makes accurately monitoring what is happening in this rich and complex ecosystem practically very difficult.

b. The consequences of inaction

That it is somewhat expected or difficult is not a reason to accept this state of affairs. After all, this trust problem is corrosive in other ways that go beyond delivering value for the industry's internal stakeholders.

Fraud is one such example. There have been some good success in reducing measurable Fraud and the UK is, relatively, a leader in this battle. But it is difficult to be too comforted in the information vacuum we find ourselves in. When you don't even know *how* all the impressions are being served, you simply can't know how much fraud there really is. We know the vast majority of organisations in this industry are trying to do the right thing. But there are simply far too many gaps in our knowledge to be sure that everyone is playing by the rules.

Consumers are directly impacted in other ways by these gaps in our knowledge. The recent AA study into consumer trust in advertising showed that public's trust in our industry has declined significantly since the 90s - to almost half what they were. It is probably no co-incidence that this period coincides with the vast explosion of digital advertising. With this technology we can reach people in more ways than ever before, sometimes on a 1:1 basis. But precisely because our messages and tactics are so numerous and individualised, it is much harder to know when they are getting out of hand. While the public is concerned about all mediums of advertising, many of the public's biggest concerns are centred around issues with particular risks in digital advertising. In digital, we have some very powerful tools that can cause particularly aggressive forms of the problems identified by the report: bombardment, intrusiveness or potentially predatory targeting of vulnerable individuals. Without a better mechanism for seeing how individual impressions are being served, it is not obvious how we would begin to protect people from these kinds of issues with a high degree of effectiveness.

Transparency is also increasingly a concern for governments - especially when it regards the power of larger market participants. In its final report into "online platforms and digital advertising" the CMA - the UK's competition regulator - has raised the concern that a lack of transparency threatens fairness in the industry altogether. They fear it might give some companies too much of an information advantage that they can exploit for their own ends. Understandably, the CMA now believes that ***"there is a strong argument for the development of a pro-competitive regulatory regime to regulate the activities of online platforms funded by digital advertising".***

For many years digital advertising in the UK has been mostly self-regulated. Government is now judging that we may no longer be up to the task of keeping it that way. For those that believe self-regulation would be the best outcome for everyone, time seems to be running out; unless things can finally change.

c. What is the solution?

Ultimately, we actually want something simple: the ability for market participants to get access to relevant impression data easily, see what is actually going on and have confidence that other relevant parties are seeing the same thing. Essentially what is missing in our industry right now is ***shared truth***: A single, harmonised record of every impression in the advertising supply chain, agreed-on and accepted by all counterparties.

It's always been TAG/JICWEBS' remit to deliver trust and transparency to the digital ad trading market: to shine a light on the dark areas. Up to now, we have done that through certification schemes. These have been based on a mixture of self-attestation and traditional audit practice: in which market participants' compliance with good business practice is regularly investigated and tested by independent auditors like ABC.

We are proud of our record on using these tools to successfully increase standards across the industry, but we also recognise these kinds of tools have limits. They can promote good behaviour, but they can only tackle the lack of *shared truth* in the most piecemeal fashion.

That is why we believe the right way forward is to solve this problem at its root: sooner rather than later. This means creating an actual *system* where shared truth resides. Not just a set of standards, but a secure always-on distributed ledger network where impression data can be stored, shared, agreed-upon and - most crucially - measured in near real-time. With such a network in place - accessible across the industry and run by the industry as a consortium - we can enforce higher standards and build the trust in the supply chain that we need.

The network will, in particular, allow to consistently enforce the legal T&C's and the requirements around impression data that an industry task force is working on following the publication of the ISBA/PwC study.

These are difficult times for media: we're in the midst of a pandemic, with an unprecedented challenge for many organisations in our industry that follows. But the trust problem is not going away. And by solving it we can actually make a more efficient, better functioning market for everyone. That's why we believe the time is right for DLT.

3. How an industry-wide distributed ledger network would solve the trust problem

We believe that only an always-on technology solution that ensures permanent access to consistent impression delivery data can increase accountability and solve the trust problem. After evaluating different solutions, we identified the creation of an industry-wide **distributed ledger network** as the best way to deliver this.

At the heart of such a network is a distributed ledger. You can think of a distributed ledger as a type of database that multiple organisations use to share data between each other. But unlike a conventional database, none of them has full control over it and they agree what makes an authoritative record by an automated consensus mechanism - rather than simply trusting the organisation that runs the database to make sure its records are reliable and secure. Since a distributed ledger isn't managed by a single organisation it doesn't have a single point of failure. Overall, it is much less prone to failures, cyberattacks and fraud.

Imagine, if all impression delivery data across an advertising supply chain was reported on and securely stored in such a ledger. Imagine also that any supply chain participant had access to that ledger on a need-to-know basis and that all the data was stored in a common format with matched impressions between participants. Imagine that all those impressions records were attributed to the legal identity that reported them and - once added - became *immutable*: they could no longer be modified. Lastly, imagine that the database supported "smart contracts" - a type of software programme that allows automatically monitor, execute and/or enforce the agreed terms. These contracts could be used to define rules for reconciliation in advance and then automatically execute those rules.

Such a network would be a single source of truth for impression delivery for the whole industry. It would drastically reduce the amount of work required to get data from different parties, reconcile impressions, increase the consistency of the data and provide proof of that data's authenticity. *Unlike* traditional databases, it would be uniquely capable of creating trust in its contents, avoiding the "garbage in, garbage out" problem:

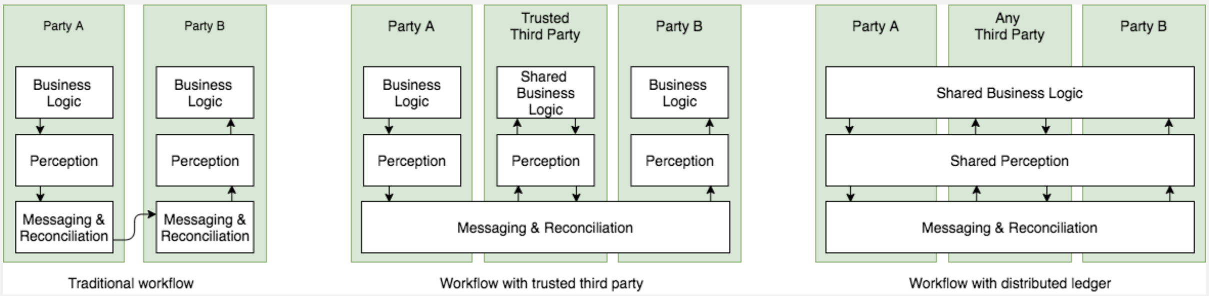
- Because of the impressions' data immutability, the network would have a tamper-proof audit trail that preserves evidence - **you would know what happened**
- Because the impression data would only be written by authenticated members, it would always be possible to trace back to the organisation that wrote the data - **you would know who reported it**

- If parties use a smart contract to define what properties a successfully delivered impression has (ie. a "qualified impression") then they would have total alignment on impression reconciliations - **you would agree on what to count**.

This combination - immutability, authentication and agreement - would give all members of this network the confidence to know that **"what you see is what I see"**: that they share an account of what happened that they all accept as authoritative. That's what would make it *shared truth* not just shared information that simply pooling data alone could bring.

Such a network is exactly what we are proposing to create: **THE TAG DLT Industry Consortium Network**. An industry wide distributed ledger network created "for the industry by the industry".

Distributed ledgers compared to traditional workflows



This diagram illustrates how differently organisations would transact using such a network versus other more traditional workflows:

- **Traditional workflow** - where parties record and manage their own impression records and have to resolve associated discrepancies manually. e.g. a very simple direct media buy between two companies.
- **Workflow with a trusted third party** - where parties delegate the recording and management of impressions records to a centralised third party who is trusted by both parties to be authoritative. Discrepancies have to be resolved manually and may require a single party to simply accept what they believe is an unfair result without being able to scrutinise data. e.g. like an agreement to invoice based on an Ad servers' impression count.
- **Workflow with distributed ledger** - where parties collaboratively record and store impression records consistently for all parties based on pre-defined rules. Discrepancies are automatically resolved.

a. Why a distributed ledger is the best option to solve the trust problem

There are many positive initiatives that are trying to solve the trust problem in digital advertising. All of these initiatives should be supported and furthered. But unfortunately, none of them provide a comprehensive solution to the problem of having a single consistent and accountable picture of what is actually happening in the supply chain.

IAB Tech Lab initiatives - like ads.txt, sellers.json and the SupplyChain object - enable ad-tech vendors to fight fraud and have greater transparency into supply chain structure. They are great initiatives, which already demonstrated their ability to decrease the level of fraud. But on their own, they can't solve the problem of trust in the industry, as they aren't dealing with the issue of independent access and verification of the impression delivery data. Certifications and audits promote good practice and behaviour, but for the most part only provide a snapshot. Given the complexity of the advertising supply chain a company can quite easily demonstrate one thing in the context of an audit and do something else the rest of the time.

This is why we believe an industry-wide distributed ledger network is the best-known solution to our problem.

- Open governance - The distributed ledger network is openly governed by a consortium of industry representatives. It balances the needs of industry participants in a transparent fashion and promotes a competitive environment - which centralised solutions controlled by single entities will not promote.
- Legal enforceability - Shared data stored in the network can be legally binding and readily accepted as admissible evidence under English law. This has recently been confirmed by the Law Tech Delivery Panel formed by the UK government. Such a footing can't be achieved by simply passing log files from one party to another because it lacks the required security. Today, if an intermediary reports different impression data to buyers and sellers in a transaction, it will be very challenging to establish any log-level evidence of this issue as admissible. Distributed ledger technology, on the other hand, guarantees that any data shared through the network is attributed to its source legal entity, is authenticated and cannot be modified - giving it a strong legal footing.
- De-duplication of legal efforts - All parties on the network sign-up to membership agreements. Part of these define how they will grant access to data quickly to each other and make smart contracts to reconcile impressions according to pre-established rules. This massively reduces the legal efforts involved compared to the current situation where separate contracts must be made with each party. The simplicity and clarity of this arrangement can increase trust.
- De-duplication of integration efforts - Because the Distributed ledger network is designed to be a single shared database and single system-of-record with a single access point it drastically reduces the integrations required. Once even a few parties

are on-boarded, it will be much faster for organisations to get access to this data and move more quickly to trust. A purely ad-hoc approach based on sharing of log files might struggle to reach the same level of adoption due to the friction involved.

- **No data exposure to intermediaries or central parties -** Data in digital advertising is often a competitive advantage and so very sensitive for all stakeholders. Because the distributed ledger network ensures sharing of the data is on a need-to-know basis and consensual basis, there are no central parties, administrators or intermediaries, that can see the data. We believe that it is highly unlikely that many industry stakeholders will be ready to delegate this task to any kind of trusted centralised party. This is why we believe that an attempt to solve the problem shared truth addresses with an industry-wide centralised database is not a realistic option.
- **How the network automates terms agreed in contracts can promote trust** - The rules embedded in smart contracts are automatically applied at the impression level based on objective criteria, agreed in full in advance. This secure automation of reconciliation promotes trust by leaving no room for interpretation and disagreement.

Here's a comparison, outlining unique advantages of the distributed ledger network vs other approaches:

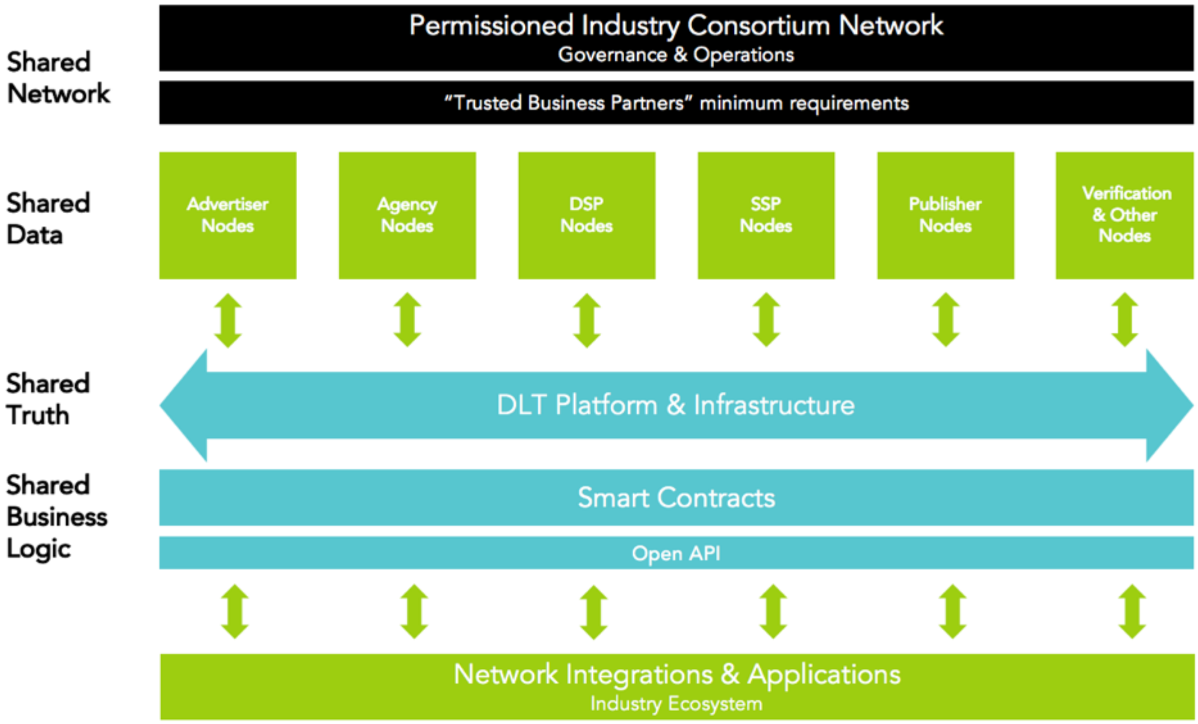
System design	Distributed Ledger Network	Centralised Database	Log Files with Common Standard
Open governance - Consortium governance, balancing the needs of participants in a transparent fashion.	Y	possible	possible
Identity authentication - Every network member is tied to a real-world legal identity, so you always know who you are transacting with.	Y	Y	possible
Data authentication - All data written by members is authenticated, so you can trust who the data actually came from.	Y	Y	possible
Data immutability - Once data is written to the network's ledger, it cannot be changed, so you can trust the record hasn't been tampered with - it always remains trustworthy.	Y	N	N
Reliability / Security - No single point of failure, established fault-tolerance and security by design.	high	medium	low
Data privacy / "Need-to-know" by design - Because data is only shared with who a participant chooses via	Y	N	N

System design	Distributed Ledger Network	Centralised Database	Log Files with Common Standard
consents and access policies with end-to-end encryption, participants remain in 100% control of their data, so they can trust it is only ever seen by the right eyes. No data exposure to intermediaries and central parties.			
Smart contracts / "What you see is what I see" - Because data can be automatically reconciled between different parties according to pre-agreed smart contract rules, there is no disagreement about facts - you have the same version of the truth.	Y	N	N
Single integration - Because you can source data from multiple parties from one place, you don't need to keep building integrations, making it faster to get to data.	Y	Y	N
Single master agreement and unified consent/access management - Because permissions are granted through software based on single master agreement, the process to provide data access consents between participants is very straightforward and easy.	Y	possible	N

b. How it would work in practice

First the network would have a governing body. This could be a consortium committee or other entity with representatives from and/or ownership by trade bodies. This governing group would define the governance policies of the network, balancing the needs of industry participants in a transparent fashion. It would specify how access to data is granted and what the minimum requirements would be to join the network. These might include supporting certain industry standards, common log file naming conventions, the need to install specific software or even agreement to arbitration in case of disputes. An operating entity (we propose TAG) would manage admission on behalf of the governor, promote the network and look after its day-to-day management. The operator would maintain direct relationships with all network participants and ensure that they use the network in line with the principles and requirements defined by the governor entity.

Here is a representation of the network's constituents:

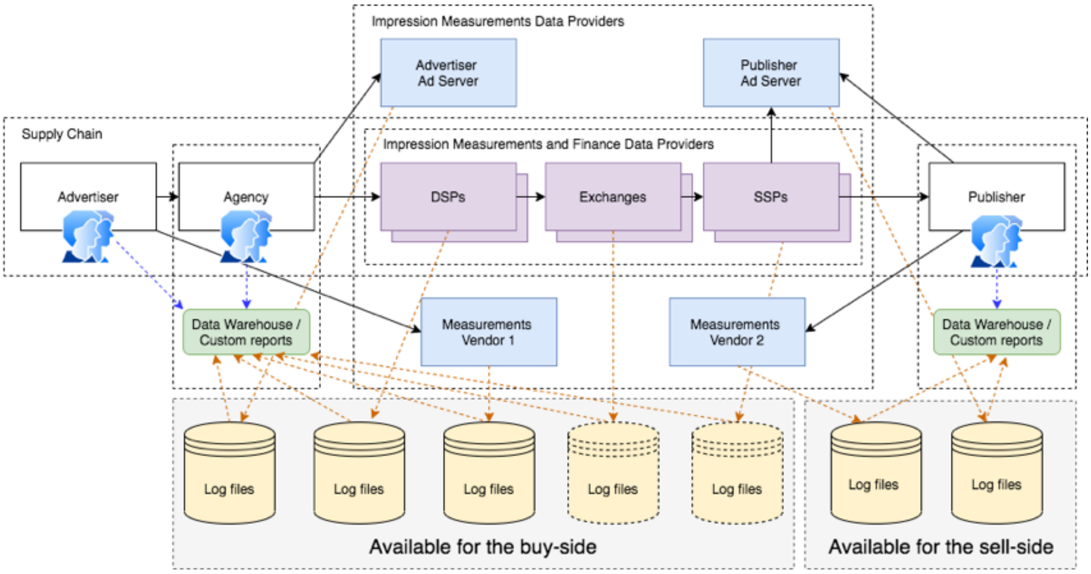


With governance and operations established, supply chain participants - advertisers, agencies, tech vendors and publishers - would install the network's platform components (or enlist other participants to install and run them for them):

- A Reconciliation SDK – client-side software that creates map of vendor-specific impression IDs every time an impression delivery process is started, which is then shared with all participants so they can deterministically match their log records even if they don't have common log file record IDs.
- A Network Node - isolated computing instance with a platform software that allows participants to harmonise and write their impression data to the network in a unified format, manage data access permissions, read impression data, reconcile it, export it to a data warehouse and run smart contracts with other participants. A Network Node allows to use the platform API to power various applications, ranging from analytics dashboards and bidding optimisation to the automation of insertion order invoicing.

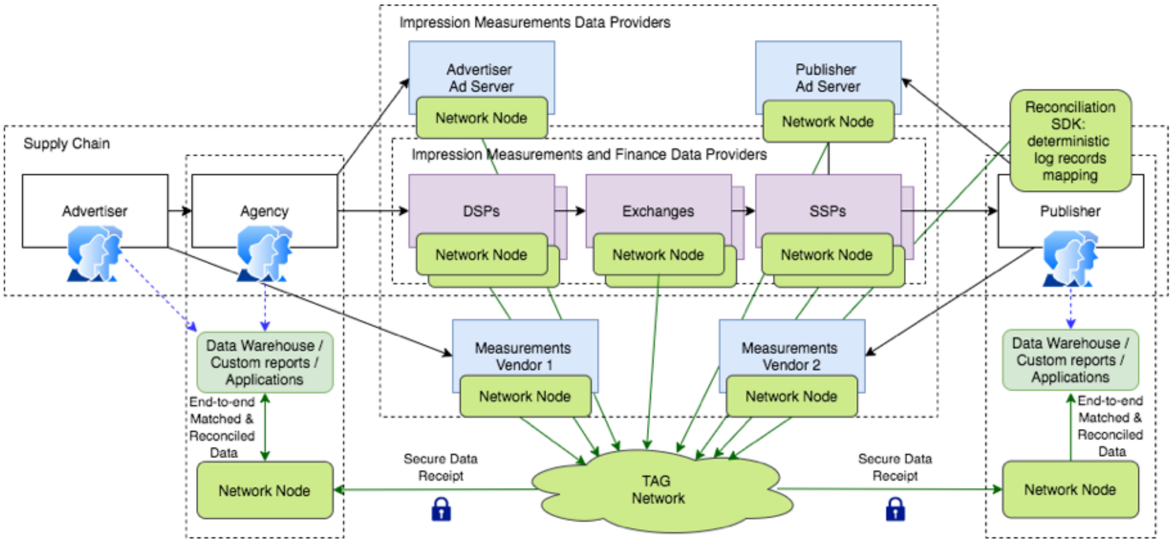
These components enable network participants to share data over the network securely and begin reconciling impressions in a much more efficient manner than today.

Today, not all parties provide logs. Where they are provided, they are often in very different formats and are not necessarily compatible with each other:


Impression Measurements Data Providers
Advertiser Ad Server
Publisher Ad Server
Supply Chain
Impression Measurements and Finance Data Providers
Advertiser
Agency
DSPs
Exchanges
SSPs
Publisher
Data Warehouse / Custom reports
Measurements Vendor 1
Measurements Vendor 2
Data Warehouse / Custom reports
Log files
Log files
Log files
Log files
Log files
Log files
Log files
Available for the buy-side
Available for the sell-side

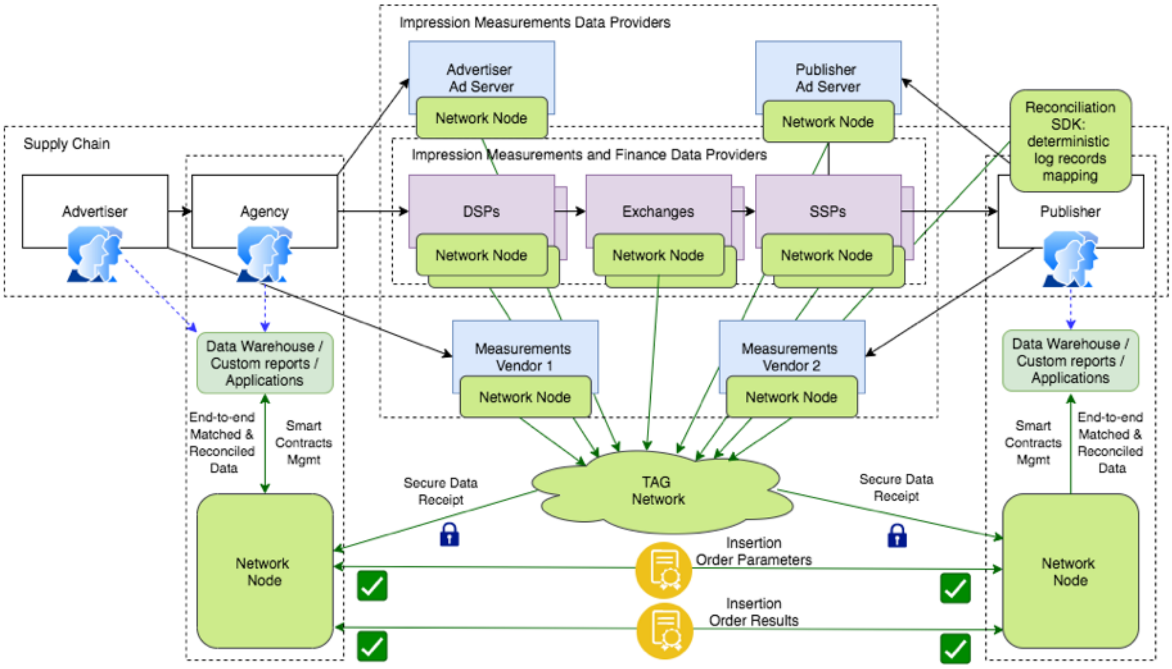
Even if some parties receive some of the logs, they don’t necessarily have them all, leading to the buy and sell sides having differing pictures of the same events. Even worse, a common record ID is often lacking, making impression data matching impossible.

With the network in place, however they will all be using the ledger as a single source of shared truth where all data has already been matched and harmonised to a common format:


Impression Measurements Data Providers
Advertiser Ad Server
Network Node
Publisher Ad Server
Network Node
Reconciliation SDK: deterministic log records mapping
Supply Chain
Impression Measurements and Finance Data Providers
Advertiser
Agency
DSPs
Network Node
Exchanges
Network Node
SSPs
Network Node
Publisher
Data Warehouse / Custom reports / Applications
End-to-end Matched & Reconciled Data
Network Node
Measurements Vendor 1
Network Node
Measurements Vendor 2
Network Node
Secure Data Receipt
TAG Network
Secure Data Receipt
Data Warehouse / Custom reports / Applications
End-to-end Matched & Reconciled Data
Network Node

Then by making a smart contract with other participants (say through an insertion order), they can agree criteria which will define the impressions to be counted as successfully delivered: the *qualified* impressions.

These criteria could include whether the impressions were rendered, how it was measured for viewability, brand safety, invalid traffic risks, dwell time, the validity of standards like ads.txt, detected discrepancy and finance data.



Once this smart contract is applied, they can come to an instant automated agreement on how impressions should be reconciled. This could even automatically generate invoices through billing software. Where there is a dispute to resolve, both parties would have access to trusted immutable records in the ledger that could be presented to a third-party auditor.

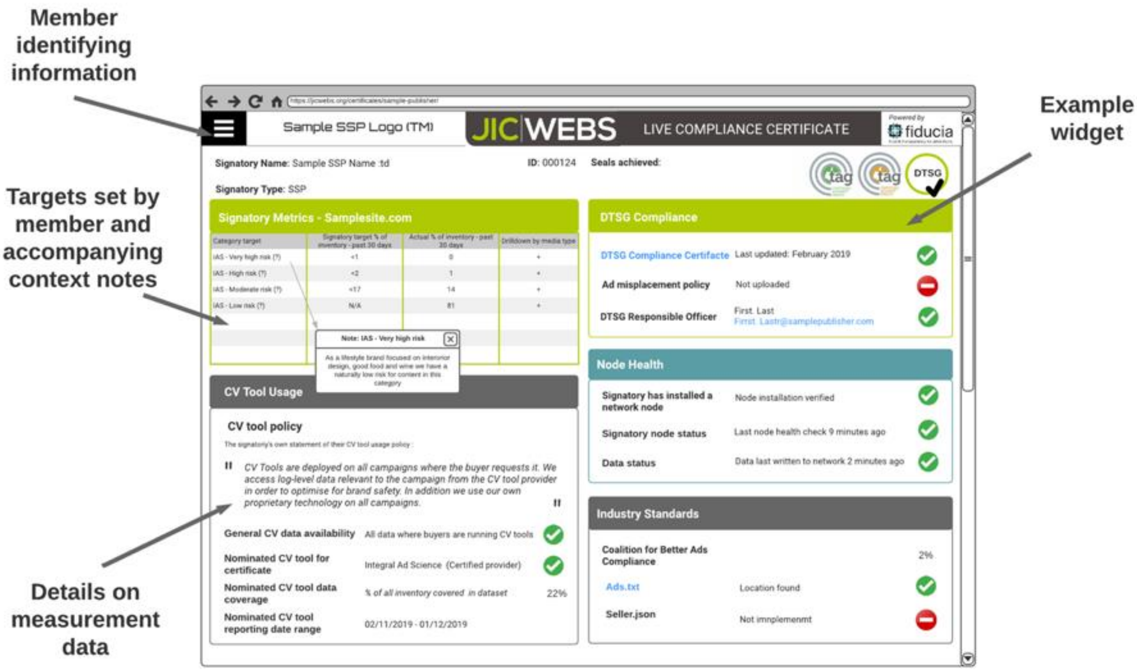
With this workflow in place, a range of different organisations could then provide new or upgraded products and services powered by this "operating system": automated billing systems, data visualisation and analytics products, AI-driven optimisation to name only a few. This would create an entirely new, competitive environment in which there would be business opportunities for a wide range of organisations.

c. Live Compliance: the network's visual interface

Live Compliance is a window into the TAG network itself. It is a searchable database of every network member that allows any registered user to see all of any member's critical compliance information on a single page we call a "Live Certificate". Its admin panel also allows network membership to be managed by TAG, and where organisations will manage their own membership settings, domain ownership records, access policies for their data and upload key documents.

The member's live certificates not only contain a record of all of these organisations' offline certifications and documentation, but they also show something not possible today: a live picture of their current compliance status. This is displayed through a series of constantly updated widgets: their current or historical performance against key target metrics like brand safety, viewability, fraud, discrepancy rates or the status of installed files like ads.txt or sellers.json or how recently they wrote data to the network. Because DLT allows access to all of this data, it also incorporates real-time alerts which can be configured by Live Compliance users to notify them as soon as there is a non-compliance issue in the supply chain. Historical compliance data will also be made available over the interface, allowing industry participants to see if there were any compliance issues in the past.

Below: Wireframe/mock-up of an example Live Compliance certificate


Member identifying information
Example widget
Targets set by member and accompanying context notes
Details on measurement data
https://jicwebs.org/certificates/sample-publisher/
Sample SSP Logo (TM)
JIC WEBS
LIVE COMPLIANCE CERTIFICATE
Powered by fiducia
tag
tag
DTSG

Signatory Name: Sample SSP Name :td

ID: 000124

Seals achieved:

Signatory Type: SSP

Signatory Metrics - Samplesite.com

Category target	Signatory target % of inventory - past 30 days	Actual % of inventory - past 30 days	Drilldown by media type
IAS - Very high risk (?)	<1	0	+
IAS - High risk (?)	<2	1	+
IAS - Moderate risk (?)	<17	14	+
IAS - Low risk (?)	N/A	81	+

Note: IAS - Very high risk ☒

As a lifestyle brand focused on interorior design, good food and wine we have a naturally low risk for content in this category

CV Tool Usage

CV tool policy

The signatory's own statement of their CV tool usage policy :

" *CV Tools are deployed on all campaigns where the buyer requests it. We access log-level data relevant to the campaign from the CV tool provider in order to optimise for brand safety. In addition we use our own proprietary technology on all campaigns.* "

General CV data availability	All data where buyers are running CV tools	✓
Nominated CV tool for certificate	Integral Ad Science (Certified provider)	✓
Nominated CV tool data coverage	*% of all inventory covered in dataset*	22%
Nominated CV tool reporting date range	02/11/2019 - 01/12/2019	

DTSG Compliance

DTSG Compliance Certifacte	Last updated: February 2019	✓
Ad misplacement policy	Not uploaded	⛔
DTSG Responsible Officer	First. Last First. Lastr@samplepublisher.com	✓

Node Health

Signatory has installed a network node	Node installation verified	✓
Signatory node status	Last node health check 9 minutes ago	✓
Data status	Data last written to network 2 minutes ago	✓

Industry Standards

Coalition for Better Ads Compliance		2%
Ads.txt	Location found	✓
Seller.json	Not imnplemenmt	⛔

By bringing all of these into one place, compliance processes across the industry could be sped-up. Everyone will have clear visibility into who the network members are, their real-world identity as well as their digital one which must be tied together as a condition of membership.

We expect Live Compliance certificates to evolve over time as new standards are introduced, the market itself evolves and new technology allows to drive compliance further. Some of the current planned features of Live Compliance include:

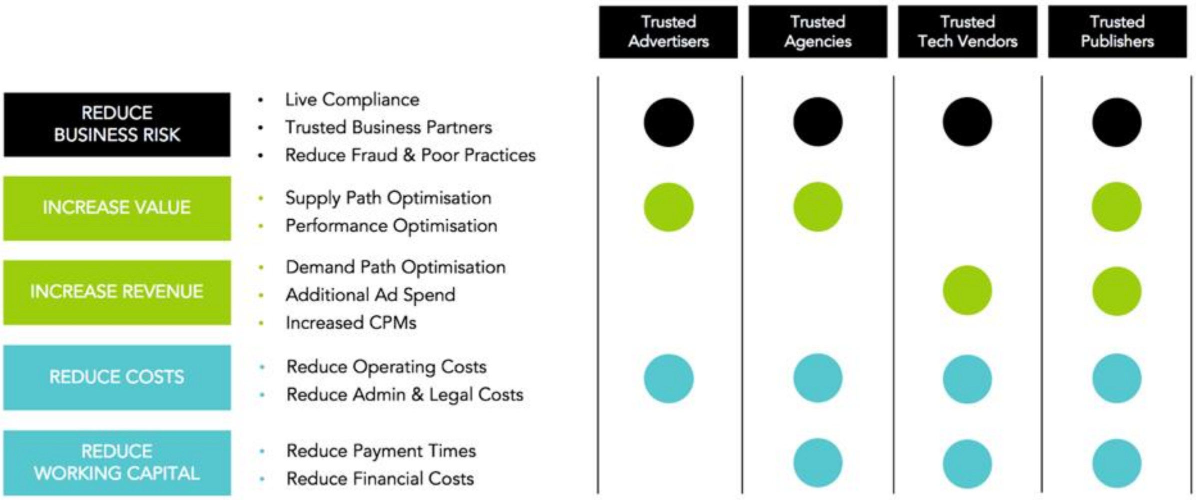
- Real world & legal identity linked to domain ownership for every member
- Configurable selection of live accountability metrics (brand safety, fraud, viewability, discrepancies or gaps in data) from a strictly curated selection determined by TAG

- Ability for suppliers to set realistic targets and better contextualise their performance against their metrics like brand safety, fraud, viewability or levels discrepancy with explanatory notes
- Ability for users to set alerts for non-compliance issues arising in their supply chain
- Filters and searches for organisations based on compliance status
- Ability to create exportable CSV whitelists from searches
- Easy-to-understand tick and cross system to show current status against key compliance criteria
- Up-to-date information on when data was written to the network
- Current versions of all contacts and policy documents for one-click downloading / review
- Admin panel for managing membership
- Admin panel for TAG

4. Benefits of the network for everyone

Together, the TAG DLT network and the Live Compliance tool will deliver a set of direct benefits to every industry participant.

Below: diagram shows some examples of the kinds of benefits different type of organisations will gain by being network members. The reduction of business risk and opportunity to reduce costs are particularly common to all participant types.



		Trusted Advertisers	Trusted Agencies	Trusted Tech Vendors	Trusted Publishers
REDUCE BUSINESS RISK	Live Compliance Trusted Business Partners Reduce Fraud & Poor Practices	●	●	●	●
INCREASE VALUE	Supply Path Optimisation Performance Optimisation	●	●		●
INCREASE REVENUE	Demand Path Optimisation Additional Ad Spend Increased CPMs			●	●
REDUCE COSTS	Reduce Operating Costs Reduce Admin & Legal Costs	●	●	●	●
REDUCE WORKING CAPITAL	Reduce Payment Times Reduce Financial Costs		●	●	●

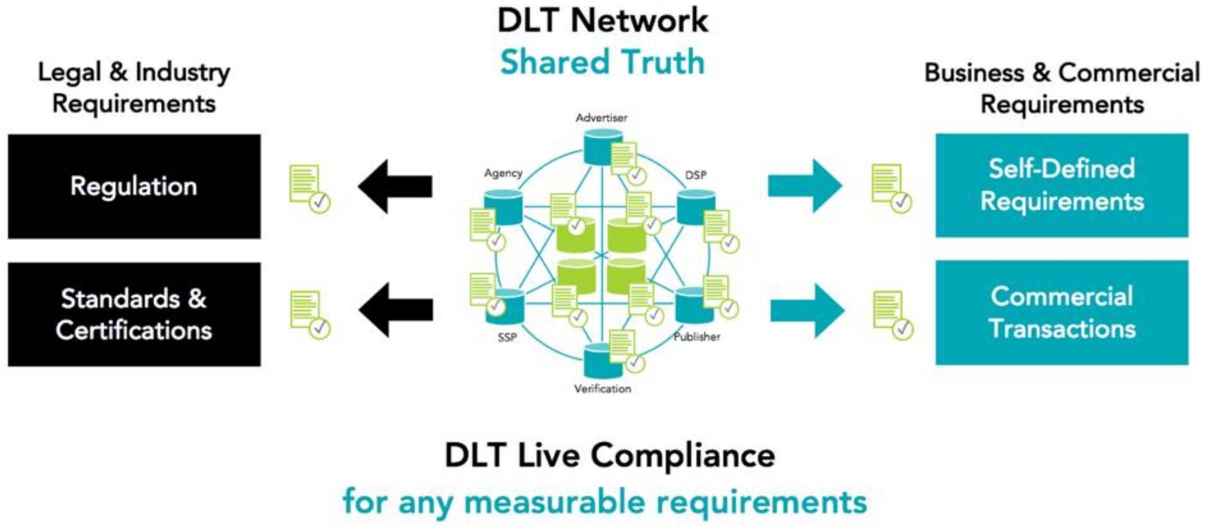
a. Reduce business risk

The network will reduce business risks in a wide variety of ways for all members of the network.

Live Compliance

Live compliance provides consistent, always-on data for advertising delivery. Industry participants can monitor each other's compliance more effectively using this tool and reduce many kinds of specific risk more effectively than one-off audit processes. By using a combination of its interface and real-time alerts based on impression-level delivery data, they can both lessen their initial exposure to risk and raise compliance problems as soon as they happen. This allows participants to lessen the impacts of these risks for themselves with a knock-on benefit across the supply chain.

Shared truth providing accountability and compliance for any measurable requirements across the supply chain:


DLT Network
Shared Truth
Legal & Industry Requirements
Regulation
Standards & Certifications
Advertiser
Agency
DSP
SSP
Publisher
Verification
Business & Commercial Requirements
Self-Defined Requirements
Commercial Transactions
DLT Live Compliance
for any measurable requirements

Examples of these risks include fraud, brand safety violations or even improper management of consumer privacy. A recent study about the IAB Europe's Transparency and Consent Framework found that out of 560 websites 54% were at least in one suspected violation of the European GDPR and ePrivacy directive. Our pilot showed that because of this capability to move beyond the limitations of traditional audits, there was already substantial interest in the deployment of the Live Compliance tool.

Dealing with trusted business partners

The network's multiple minimum requirements for entry and the high level of accountability it promotes will build a high level of trust between parties. Every new member knows that every other member of the network has already signed the same set of membership agreements to join the network and meet its high bar for good practice and reporting. This establishes all members as mutually **trusted business partners** that each other member can rely on. Not only does this squeeze out the potential for fraud, but it creates a positive incentive to work only with such trusted business partners in future - allowing them to increase their revenues and further drive better standards elsewhere.

Security & business continuity

The ledger is a highly secure way to share and store sensitive commercial data - the distributed ledger network is designed to operate under the assumption of an adversarial security environment. It includes end-to-end data encryption, integrity, authenticity and other security features required to protect the network against being compromised.

Because it is distributed and has these inherent security features, the risks of unauthorised access to critical data, breach of agreed contract rules or losing access to required data is much lower than other approaches for data sharing and storage.

b. Reduce costs

Reduction of technology costs

A single integration point with DLT allows an organisation (with proper consents) to get access to all the log file data of *all other network members*. Because the platform's unified API makes the data available in a common format, it is also ready for use in other systems - like data warehouses - without further transformation. This allows the re-allocation of resources that would otherwise have to be allocated to the build and maintenance of multiple log file integrations.

Reduction of reconciliation costs

Our pilot report verified that today significant effort is expended simply reconciling impression records between parties. According to our research, simply extracting, formatting and reconciling data consumes 59% of agency analysts' time. With DLT, all of that preparation work would be completely automated. This would allow all of this labour cost - and similar costs up-and down the supply chain - to be completely re-allocated.

Reduction of legal costs

The agreements all members sign-up to when they join the network will specify how members grant consent to each other to access data. Digital access policies managed using the Live Compliance interface will define exactly who has which consents. Smart contracts will specify exact impression reconciliation rules that will make the reconciliation processes completely automated. Arbitration requirements may be added to the membership agreements to specify how disputes would be resolved if they arise. Between these different network features the amount of legal work required to administrate these processes will drop dramatically. Records on the ledger can also be accepted as admissible evidence or be legally binding by all parties in any dispute that does arise, depending on the evolution of UK legislation. This should reduce the risk of complex, protracted legal action even more: further reducing legal expenditure.

c. Creation of a new industry ecosystem

By its nature, the network is not a single point solution, but an *enabler* across the entire marketplace. Through the platform's open API, a competitive, open environment will be created. All organisations will be free to explore different ways to drive more value from the network.

It will empower a diverse group of supply chain participants, 3rd party application developers and system integrators to better solve existing problems and exploit entirely new opportunities. Using the rich, reconciled impression data - the Shared Truth - stored in DLT and the currency of trust the network will create, they will build new products and services, and improve the functionally of existing ones. From billing platforms to new forms of AI optimisation, from analytics to financial products, the network offers a wide range of extension opportunities to develop a new industry ecosystem built on Shared Truth.

The knock-on effect of the innovation this could stimulate will benefit the entire industry through the emergence of better or more cost-effective products.

5. What are the benefits to me?

Beyond the broader benefits all participants stand to gain from the network, different types of supply chain participants will each have more unique opportunities to exploit. The following section explores some of those potential benefits.

a. Advertisers

Overall benefit: Through 3rd party applications and their own tools, the TAG DLT network will allow advertisers to increase their return on advertising spend by providing always-on visibility into the supply chain. By extension, brands can expect to increase consumer trust through improved communication opportunities, and higher brand safety and suitability standards which can be better enforced.

- Improved compliance - Because impression data is available always-on via the unified API, campaign activity can be constantly monitored for compliance. Real-time alerts can raise potential non-compliance issues as soon as they occur through the Live Compliance tool.
- Trusted business partners - Because all members have to meet the standards set by the network - including reporting their data constantly to the ledger - the network provides a clean, safe environment for advertising spend.
- Supply path optimisation - Always-on reporting into the supply chain and visibility of sell-side data will make identifying more efficient paths to inventory simpler and more effective.
- Better allocation of spend to ‘qualified impressions’ - The pilot demonstrated that, on average, 20% of analysed ad spend is attributed to impressions that weren’t ‘qualified’: those that did not meet a minimum quality requirement for discrepancies, measurability, brand safety and fraud prevention. Smart contracts can automatically reconcile impressions and verify these criteria, creating opportunities to better optimise spend.
- Cheaper and simpler access to impression data - Because the DLT is a single point of integration to get log files data, the number of log file integrations required to get access to impression data could substantially decrease. Multiple reporting sources could be consolidated, or the number of analytics platforms rationalised.

b. Agencies

Overall benefit: The TAG DLT presents substantial efficiency and cost reduction opportunities to agencies. It also provides an automated system to reduce business risks.

- **Faster, more effective compliance processes with live compliance** - Because Live Compliance brings a participant's compliance information into one searchable database - certificates, implementation of standards, real-time metrics on brand safety, fraud, viewability and discrepancies - it can increase the efficiency and effectiveness of both compliance teams and trading desks: saving costs while reducing risks. The tool's unique ability to generate real-time alerts can raise potential non-compliance issues (such as un-authorised sellers or lack of adequate user privacy policies) as soon as they occur, reducing reaction time and associated business risks, while improving client trust.
- **Cost saving on campaign reporting & reconciliation processes** - Our pilot report found that 59% of the time of agency programmatic analysts, campaign managers and technical managers was spent in reconciling data, rather than analysing it or actively resolving discrepancy issues. Because the impression data can be automatically reconciled with smart contracts and then fed directly into a billing platform, substantial labour cost of up to 21% could be saved. 52% of respondents to research carried out as part of the pilot, thought campaign reporting and reconciliation would benefit most from automation.
- **Cheaper and simpler access to impression data** - Because the DLT is a single point of integration to get log files, the number of log file integrations required to get access to impression data could substantially decrease. This could realise considerable cost savings. Our pilot research showed that some single integrations with a 3rd party data source can incur a cost of up to £10,000 and recurring fees that are passed on to the end data user. Between 15 to 20 such integrations would be required for the average large client.
- **Complement or augment existing data initiatives** - Since the DLT simply provides access to a reliable, reconciled impression data set, it could be used to augment existing business or campaign intelligence projects - feeding data directly into data-warehouses or client-facing data visualisation tools.
- **Legal enforceability of records and ease of availability for audit** - Because of a common legal framework, smart contracts and immutability, records could be used as indisputable evidence and made available instantly for audits.
- **Reduction in legal costs** - The estimated 15 to 20 integrations required per client each require a different contract for data to be provided. The single master service agreement (MSA) of the DLT network, and the system for providing access to data under this agreement, removes the need to have separate and bespoke contracts. This would considerably reduce the amount of legal administration involved and decrease risk in the process.

c. DSPs and SSPs

Overall benefit: The TAG DLT network could enhance many aspects of existing DSP and SSP product offerings, help respond to the industry's requirement for greater trust and transparency and improve efficiency.

- An effective way to respond to the industry's call to action on trust & accountability The DLT is a cost-effective and secure way to share data that can be harmonised through the supply chain, demonstrating compliance, accountability and cementing an organisation's role as a trusted business partner.
- Augment data portability initiatives - Because the DLT platform is built to share log-level impression data between parties, it could simplify the infrastructure needed to share data, provide new functionality and ultimately allow more businesses to work with the data.
- Create Efficiencies and Reduce Costs - The DLT platform can be used to store and share data reducing logging costs. It also provides access to unified data from parties, both up-stream and down-stream, that can be used to support discrepancy management, reconciliation or to enhance existing bidding, targeting and reporting solutions. It can also greatly reduce the time and legal resources spent on delivering consents between participants.
- Faster, more effective compliance processes - Because Live Compliance brings a participant's compliance information into one searchable database - certificates, implementation of standards, real-time metrics on brand safety, fraud, viewability and discrepancies - it can increase the efficiency and effectiveness of compliance processes. The tool's unique ability to generate real-time alerts can raise potential non-compliance issues (such as un-authorised sellers or lack of adequate user privacy policies) as soon as they occur, reducing reaction time and associated business risks, while improving client trust.
- New targeting and reporting products - New targeting options could be provided that allow clients to buy or sell only inventory from trusted business partners, target sites that meet certain criteria with their Live Compliance certificates or comply with particular custom criteria.
- Campaign configuration data availability - Using the network, all brand, KPI, verification targets or settings could be automatically provided from advertisers or agencies to all tech vendors in the supply chain, including sell-side ones, allowing them to better deliver campaigns. This information would be attached to a smart contract and be delivered securely through the network, reducing the current information asymmetry and giving all participants the ability to optimise and deliver performance.

d. Publishers

Overall benefit: The TAG DLT network would give publishers the ability to more effectively monetise inventory by demonstrating commitment to trust and enhancing their knowledge by getting access to the buy-side information.

- **Increase revenues by demonstrating quality and trust** - A publisher's Live Compliance certificate can demonstrate their superior commitment to quality and good practice to buyers. As trusted business partners they can drive increased CPM yield over their competitors, strengthening their market position.
- **Properly contextualise metrics used by buyers to increase yield** - Each publisher has a unique environment for advertising which can sometimes be undervalued or exploited by overly blunt buy side metrics or blocking measures. This prevents them from monetising quality content. A publisher's Live Compliance certificate can allow publishers to overcome this problem. First, the certificate allows them to choose which metrics - from a fixed selection curated by TAG - best represent their inventory and set targets against them. Second, it allows them to contextualise their results against those metrics by providing explanatory notes. This gives buyers a much clearer grasp of what exactly they are buying, giving them the confidence to trust more of a campaign's care to individual publishers instead of relying on very cautious blocking settings.
- **Improved optimisation capabilities** - Publishers will have easier access to data that can be effectively used in their demand-path optimisation applications, resulting in better yields and higher CPMs.
- **Campaign configuration data available** - Using the network, all brand, KPI, verification targets or settings could be automatically provided from advertisers or agencies to all tech vendors in the supply chain, including sell-side ones, allowing them to better deliver campaigns. This information would be attached to a smart contract and be delivered securely through the network reducing the information asymmetry which currently exists and giving all participants the ability to optimise and deliver performance.
- **Improved access to financing options** - Organisations could gain access to credit directly against smart contracts. New finance applications could use these smart contracts to automatically provide invoice financing resulting in faster payment times.

e. Verification vendors and ad servers

Overall benefit: The DLT network would augment existing data portability initiatives and open-up new revenue lines.

- **An effective way to respond to the industry's call to action on trust & accountability** The DLT is a cost-effective and secure way to share data that can be harmonised through the supply chain, demonstrating compliance, accountability and cementing an organisation's role as a trusted business partner.

- **Augment data portability initiatives** - Because the DLT is built to share log-level impression data between parties, it could simplify the infrastructure needed to share data, provide new functionality and ultimately allow more businesses to work with the data.
- **Create efficiencies and reduce costs** – The DLT can be used to store and share data reducing logging costs. It also provides access to the unified data from parties, both up-stream and down-stream, that can be used to support discrepancy management, reconciliation or to improve existing targeting and reporting solutions. It can enable new product offerings and greatly reduce the time and legal resources spent on delivering consents between participants.
- **New revenue opportunities** - A key feature of Live Compliance relies on measurement companies providing an independent measurement of overall supplier performance. Network participants need to have access to the measurements data to enable display of respective metrics. This presents an additional business opportunity for verification vendors. The simplicity of passing log-level data via DLT creates more potential opportunity to sell access to critical verification data in general.

f. Third party application providers and system integrators

Overall benefit: The DLT network will create a wide range of new business opportunities for 3rd party application developers, system integrators or other service providers.

- **Possibility to build a wide range of solutions for the industry** - Media insertion orders/billing tools, data visualisation and analytics, supply chain intelligence, AI-based optimisation, credit risk management, invoice financing, clearing and settlement automation to name a few.
- **Reduction in time-to-market and time-to-customer value** - Because high quality well organised data is already available for export through the DLT network's single API, deploying highly functional applications will be much quicker compared to ecosystems in which much work has to be done assembling the data.
- **Lower cost of delivery** - The robustness, flexibility and simplicity of the DLT enables greater focus on the core value of applications and potentially decreased the cost-of-build and delivery, leading to greater margins.
- **Trustworthy, high quality datasets** - Permissioning of trusted business partners based on minimum requirements coupled with data security and immutability naturally leads to higher quality datasets that are likely to be very useful for both audit trail keeping and prediction.

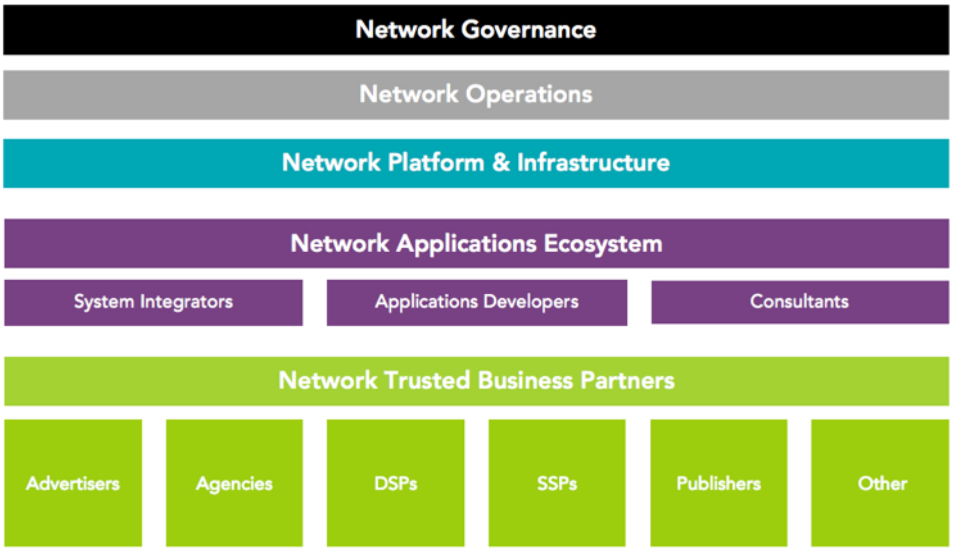
6. The network structure and organisation

The creation of a collaborative environment such as a DLT network can occur in different ways and for different reasons, but they all tend to implement similar organisation structures. As an industry consortium network, the TAG DLT initiative requires a well-defined organisation with a clear set roles and responsibilities. It needs to provide the right balance to address the needs of all industry participants and the conditions for fair competition based on a set of rules that get enforced consistently – which centralised solutions do not offer.

The TAG DLT network is to be composed of:

- A **Network Governor** – The entity responsible for the network governance.
- A **Network Operator** – The entity responsible for membership management and enforcement of the policies established by the governing entity.
- The **Network Platform & Infrastructure Provider** – The entity responsible for providing the software solution and infrastructure to "power" the network.
- The **Network Applications Ecosystem** – All the organisations developing applications or providing value added services to network participants.
- The **Network Participants** - All the organisations complying with minimum network requirements and using the platform to share impression data and make use of the services offered by the network.

These components together **are** the network.



a. The Network Governor

The network governance entity is responsible for defining the strategic management and governance policies of the network. It is also accountable for the ongoing implementation and enforcement of those policies.

The network governance entity is in particular responsible for:

- **Defining the legal and regulatory basis** on which the network is set-up and operates.
- **Setting the governance guidelines for the network**, the overall framework for how the network will be governed (the Corda network guidelines, a consortium network run by the Corda foundation, are a good example).
- **Deciding eligibility criteria for joining the network**, what minimum requirements the candidates must have achieved to join, and thus become a trusted business partner.
- **Creating the financial model** that sustains the network operations and considers its growth. *The network financial model will be defined after the Consultation process as part of the MVE phase.*
- **The membership agreements,** including a master service agreement (MSA) all members must abide by and creating the basic legal framework for using the platform, for granting permissions to access data, for the implementation of smart contracts or for disclosing information over the Live Compliance solution.
- **Determines how the network is operated and supported**, including membership on-boarding and off-boarding requirements, network parameters, as well as any dispute management rules and processes.

The industry already has trade bodies acting as representatives of the different supply chain constituents. These bodies already have defined standards, certifications and best practices for the industry that the network would help to enforce. As a result, they are in the best position to act as the governance entity.

It provides the guarantee for the network to be set-up and managed in the best interest of the industry as a whole. As a joint initiative, it will also ensure wide adoption, encouraging any company "willing to resolve the trust problem" to join the network.

The detailed structure of the governance entity remains to be defined. It is to be formed by representatives of the trade bodies and representatives of their members as required or deemed appropriate.

Determining the exact make-up, structure and role of this entity is a key part of the MVE. We particularly welcome feedback and input on this subject.

b. The Network Operator

The network operator it the entity responsible for membership management and the enforcement of the policies established by the governing entity.

The network operator's main responsibilities include:

- **Implementing and enforcing policies** established by the Network Governor.
- **Membership evaluation and authorisation,** evaluating applications and granting permissions when candidates comply with the minimum requirements set by the Network Governor
- **Driving network adoption and retention**, handling marketing, promotion, and any other day-to-day organisational services, that are required to operate a healthy industry network.
- **Monitor network participants,** ensuring always-on compliance with minimum requirements via the Live Compliance solution**,** making sure participants are following the rules of the network.
- **Managing legal agreements**, manage all legal agreements with network participants, technology providers and any other third party where there is a need to have a contractual agreement.
- **Providing reporting** to the Network Governor.

TAG already manages a certification membership programme and the consistent implementation of rules with cross-industry recognition. Given this and the network's goal in driving "live compliance", the network operator role aligns with TAG core competencies. As a result, TAG is well positioned to become the network operator. It is planning to have a dedicated team to take on these responsibilities.

c. The Network Platform & Infrastructure

To make the network operational it requires a distributed ledger software platform and an infrastructure to be deployed and managed by a technology company. The Network Platform & Infrastructure Provider is the entity responsible for providing this platform and infrastructure based on an agreement with the network operator.

As part of the Pilot, a DLT Evaluation Committee formed of 20 industry and blockchain experts, and representatives of each of the trade bodies was created. The Committee reviewed the pilot as it progressed, conducted a comprehensive process to evaluate the offering of different technology providers and made a recommendation on the selection of the provider. An important requirement was for the provider to be exclusively focused on the development of a DLT platform for the digital advertising industry and not developing applications for any particular part of the supply chain to avoid conflicts of interest with industry stakeholders.

Based on the assessment of a number of distributed ledger solutions and providers and the analysis of the requirements, the DLT Evaluation Committee recommended for the UK company Fiducia DLT Ltd to be the platform and infrastructure provider. As such, the Fiducia platform is to become the "operating system" of the network and the distributed ledger software that powers it. It provides the core network functionalities and includes the software that runs on every Network Node writing data to the network or reading from it. *This is further documented in the Pilot Interim Report and in the Technical Document.*

Fiducia was founded in the UK in early 2019 after a two-year technology development cycle for the specific purpose of providing a DLT platform for the digital advertising industry matching industry needs. Fiducia continues development of its high frequency DLT platform and demonstrated its practical readiness to process data volumes at a scale required for the programmatic advertising marketplace, as well as capabilities of end-to-end data privacy protection and usage of smart contracts for automatic advertising insertion orders reconciliation between multiple parties.

The Fiducia platform is the only platform known to us, which is built on top of the leading enterprise distributed ledger software Corda, widely used in various industries by distributed ledger networks including banking and insurances. Importantly, the Fiducia platform implements a technology design allowing to operate the network with usage fees to remain below 1% of the advertising spend running through the network. This 1% represents a small fraction of the expected efficiency gains, as already validated by the Pilot.

A fair business model for all stakeholders - based on their contributions and benefits, is to be finalised as part of the MVE after the consultation process.

Here are some of the key Fiducia platform principles:

- Interoperability:
  - Single API. Multiple applications can coexist and interoperate on the same network using the platform's API.
  - Single Data Format. Fact records on advertising impressions shared by network participants are harmonised to a single extendable format, which ensures unambiguous interpretation.
  - Corda. The network is based on the Corda distributed ledger software and is interoperable with the Corda networks deployed across various industries.
- Scale. The network is scalable to process data volumes inherent to the programmatic advertising marketplace.
- Privacy. All information in the network is shared on a "need-to-know" basis, so that the only parties with legitimate access rights can see the data.
- Automated Data Access Consents. The network participants are able to manage their consents for advertising delivery data access in an automated fashion.

- **Harmonisation.** The network participants are able to ingest advertising delivery data from different data sources and formats by using pluggable data connectors, which harmonise data to the unified formats used by the network.
- **Matching.** The network participants are provided with a Reconciliation SDK, which allows deterministic matching of impression delivery records across the supply chain by building and logging vendor-specific log record ID maps.
- **Security**. The network is designed to operate securely even in a hostile environment, ensuring end-to-end data encryption, integrity, authenticity and other security features required to protect the network against compromise.
- **Reliability.** The network is designed to operate with fault-tolerance and disaster recovery processes, minimising network availability risk.

R3/Corda – Market leader in enterprise blockchain

In its top blockchain predictions for 2020, Outlier Ventures predicts that "Corda will overtake Hyperledger, Ethereum, and Quorum by market share and become the market leader in enterprise blockchain."

Corda is an enterprise DLT software firm working with a broad ecosystem of more than 300 participants across multiple industries from both the private and public sectors, developing DLT platforms and applications on Corda software.

Working alongside the world's leading financial institutions, R3 made a conscious decision in 2016 to leverage DLT technology to solve real business problems in both complex and highly regulated markets. Today, R3 has transformed from a bank consortium to an enterprise software firm considered by many as the most robust and innovative DLT enterprise software solution on the market.

Learn more about R3 and Corda here.

d. The Network Applications Ecosystem

With a platform focused on providing the "operating system", the network will create the opportunity for anyone to use the unified API to integrate their existing systems, develop new applications, or provide value added services. This will create a wide industry ecosystem built on shared truth.

Application providers could be agencies building analytic and reporting tools, DSPs and SSPs using the API to enhance their offering, consultancy firms working on behalf of larger companies or start-ups delivering SaaS interfaces providing added value to network participants.

These applications could cover a whole range of areas providing efficiency gains in operations, finance or legal departments:

- Real-time compliance monitoring
- Supply path optimisation
- Demand path optimisation
- Bidding optimisation
- Discrepancy management
- Holistic verification
- Supply discovery
- Demand discovery
- End-to-end performance analytics and benchmarking
- Credit risk management
- Invoice financing
- Payments clearing
- Payments settlement
- Forward contracts marketplace

e. The Network Participants

The network participants themselves are companies active in the digital advertising supply chain that have been approved by the governance entity as members of the network. They benefit from all the network functionalities described in this document for as long as they comply with minimum network requirements.

The organisation structure with detailed roles & responsibilities, is to be finalised as part of the MVE after the consultation process. We welcome your input on this topic.

7. How your organisation can start using the network

One of the key design principles for the distributed ledger network deployment is the ability for industry stakeholders to adopt it in small incremental steps, requiring minimum effort.

We envision two main types of network service. Each requires a different amount of investment and providing different levels of functionality. An industry participant can choose which services are most suitable to their business requirements.

a. Network membership

This is the minimum required to join. To join and remain a member, the participant ensures continuous compliance with minimum requirements set by the network governance entity for its business type.

Participants with network membership receive a unique identity on the network and are able to manage consents and access policies for data related to them. To do that they can use the Live Compliance interface or the network's API, authenticating changes with their own cryptographic key. They won't be able to write or read data directly but can manage permissions for others to write and read data for them using this key. For example, publishers may allow ad networks and SSPs to write and read data for them.

When first joining, a Live Compliance certificate will be created for the participant. This becomes a public facing proof of membership, which anyone can access.

b. Network node

A network node is a dedicated computing instance running platform's software, which enables a member to use the platform API for direct interactions with the network. A node may be used by participant to:

- Ingest data to the network using configured data sources and harmonisation rules, ensuring data immutability and secure sharing with allowed recipients;
- Access and reconcile network data;
- Export network data to an external data warehouse;
- Set up smart contracts for the automatic reconciliation, clearing and settlement of advertising delivery between two or more parties.

Network Nodes are owned and controlled by participants and may be deployed in the cloud or on premise. Deployment and operating costs are expected to be comparatively low, not exceeding the operating costs of traditional databases.

The Network Platform & Infrastructure Provider provides an option for network participants to use isolated computing instances in the cloud environment to run their network nodes and control them using a SaaS interface suitable for non-technical staff. Network participants may also decide to delegate operations of the Network Node to a third party.

In the long term, we expect Network Nodes to be run by most or even all ecosystem participants, including third party application providers.

The differences between the described network services is summarised below. This is subject to further adjustments prior to network launch.

Network Services	Basic Membership	Network Node
Verified Network Identity	Y	Y
Live Compliance page	Y	Y
Data Access Consent Management	Y	Y
Ingest Log Files and Dictionary Data	N	Y
Setup Harmonisation Rules	N	Y
Create Shared Data Feeds	N	Y
Receive Shared Data Feeds	N	Y
Reconcile Shared Data Feeds	N	Y
Export Received / Reconciled Data to Data Warehouse	N	Y
Configure Smart Contracts	N	Y
Sign Smart Contracts	N	Y
Execute Smart Contract Workflows based on Received / Reconciled Data Feeds	N	Y

c. Process to join the network

Here is the process to join the network:

Step 1: Apply to join

Participation in TAG distributed ledger network is open to any marketplace participant but is subject to meeting minimum compliance requirements set by the network governor. This includes signing a network *Master Services Agreement (MSA)* and paying participation fees to cover both the governance and operational costs of the network.

The fee structure is to be defined jointly by the trade bodies as part of the MVE after the consultation process.

The potential member will make their application through the Live Compliance interface. Several key pieces of information will be required:

- Proof of legal identity;
- Proof of domain names ownership;
- Proof of industry specifications implementation (ads.txt, sellers.json);
- Address, business names or other key legal documents;
- Member's cryptographic public key.

The Network Operator verifies these documents and checks the application against the rules set by the network governor.

If the application is successful, the applicant will get a unique Network Member Identifier (NMI) and a signed public key certificate. The participants can then use their cryptographic keys to authorise data access consents, authenticate reported data, decrypt received data, sign their records on the distributed ledger or create smart contracts.

Step 2: Configure data access consents and live compliance

Once registration is done, the participant can use Live Compliance to configure data access consents and policies. All policies are signed with the participant's key.

In addition, participants are able to configure customisable parts of their TAG Live Compliance page: such as what metrics they would like to display in their Live Certificate, what the targets are for them or additional contextual notes for those metrics.

Step 3: Setup Network Node (optional)

If the participant intends to read data from the network, write data to the network or run smart contracts, they need to install and run a Network Node instance. Network Nodes can easily be installed and operated in the cloud or on premise via the provided user interface or platform API. The main steps are:

1. Configure the participant's cryptographic keys for the Network Node;
2. If the participant intends to share data in the network, configure data source credentials together with harmonisation rules using the predefined set of data connectors, define shared data feeds and access permissions;
3. Discover available data feeds, setup their reconciliation and export to external data warehouse, if required;
4. Define required smart contracts, share them with counterparties, sign and start automatic execution;
5. Establish monitoring of system alerts for timely reaction on data and compliance issues.

Platform software includes data connectors for log files and dictionaries of major programmatic platforms, with new connectors getting added as required. Network Node harmonises the log files original format to the common format of the network. The process is rather like matching field names when uploading a spreadsheet to a CRM or email marketing tool. This is an important step, as it means that if different supply chain participants give the fields in their logs different names, or use different formats, or if they have a slightly different set of fields available, their data can still be reconciled accurately.

The harmonisation process eliminates the need for a common format or common naming convention for log files of different network participants.

8. Timeline and next steps

a. Preparing for network launch

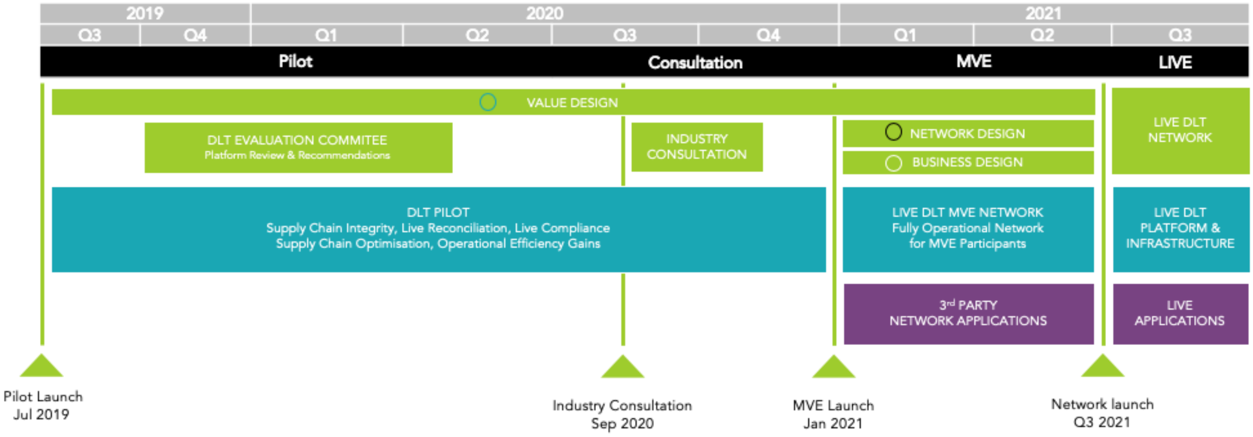
The TAG DLT Pilot has been running since July 2019 and will continue to run up to the end of the industry consultation process and the decision to launch the network.

The Consultation is the opportunity for all industry participants to get a good understanding of the initiative and to provide their input to better define network priorities. The industry input, together with the recommendation of the consultation Steering Committee, will be taken into account for TAG' decision on next steps and the launch of a DLT industry consortium network possibly by the end H1 2021.

Upon decision to move ahead, a Minimum Viable Ecosystem (MVE) will be set up. The MVE is a full 'beta' deployment of the TAG DLT Network with a limited set of participants. It is scheduled to run across H1 2021 as a fully operational DLT network with Network Nodes installed and run by the different participating organisations. The MVE will be open to application developers, system integrators and consultants as early contributors to the development of the network ecosystem.

If you are interested to know more about the MVE, please contact us. We would very much like to hear from you.

Here is an overview of the overall project timeline:


2019
2020
2021
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Pilot
Consultation
MVE
LIVE
VALUE DESIGN
DLT EVALUATION COMMITEE
Platform Review & Recommendations
INDUSTRY CONSULTATION
NETWORK DESIGN
BUSINESS DESIGN
LIVE DLT NETWORK
DLT PILOT
Supply Chain Integrity, Live Reconciliation, Live Compliance
Supply Chain Optimisation, Operational Efficiency Gains
LIVE DLT MVE NETWORK
Fully Operational Network for MVE Participants
LIVE DLT PLATFORM & INFRASTRUCTURE
3rd PARTY NETWORK APPLICATIONS
LIVE APPLICATIONS
Pilot Launch Jul 2019
Industry Consultation Sep 2020
MVE Launch Jan 2021
Network launch Q3 2021

During the MVE and before the network launch, there are several important tasks to complete. These fit into three main workstreams: **Value design**, **Network design**, **Business design**.

b. Value design

This is the process of designing *what* the network will deliver to make sure it provides value to its members. The pilot has already validated the substantial value the network provides, and the benefits trusted business partners across the supply chain will derive from it. However, we expect to refine our value design further with input from the consultation process and what we learn from the MVE. This will ensure we are fully market ready when time comes.

c. Network design

This is the process of defining the network governance and operating principles. As this document shows, we are well underway in defining how it will be structured and managed, but the principles themselves and the minimum requirements to join the network have yet to be fully discussed and finalised. They will largely be based on all the existing work done by TAG and the trade bodies to define standards, certifications and best practices. The Live Compliance solution requires additional industry input and its design will be fully validated in the MVE phase.

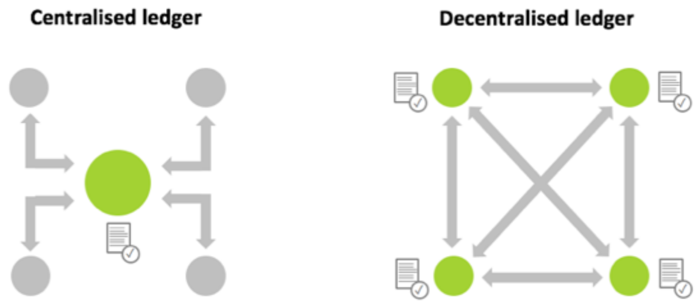
d. Business design

Business design is about defining the business model which will underpin the network. While network usage cost should not exceed 1% of the advertising spend running through the network, it has not yet been agreed how this will be broken down. It needs to be fair, with charges proportionate to the benefits each participant would receive and the costs they would incur. This is not a particular focus of the consultation process and is expected to get discussed and finalised during the MVE phase with the involvement of the trade bodies and representatives of their members.

9. TAG DLT Network FAQ

What is a distributed ledger?

It is a type of database which stores transaction records and is consensually shared, synchronized and accessible across multiple organisations, sites, institutions, or geographies. A distributed ledger stands in contrast to a centralized database, which is more prone to failures, cyber-attacks and fraud, as it is administered by a single organisation and therefore has a single point of failure.



What is distributed ledger technology or DLT?

It is technology that enables the operation and use of distributed ledgers.

What is the difference between DLT and blockchain?

The terms blockchain and DLT are often used interchangeably. Blockchain is a particular type of DLT which was popularized by Bitcoin. In Bitcoin, the ledger of transactions is as a sequence of blocks of data linked together through cryptography. The name comes from the fact that the ‘blocks’ are ‘chained’ in this fashion.

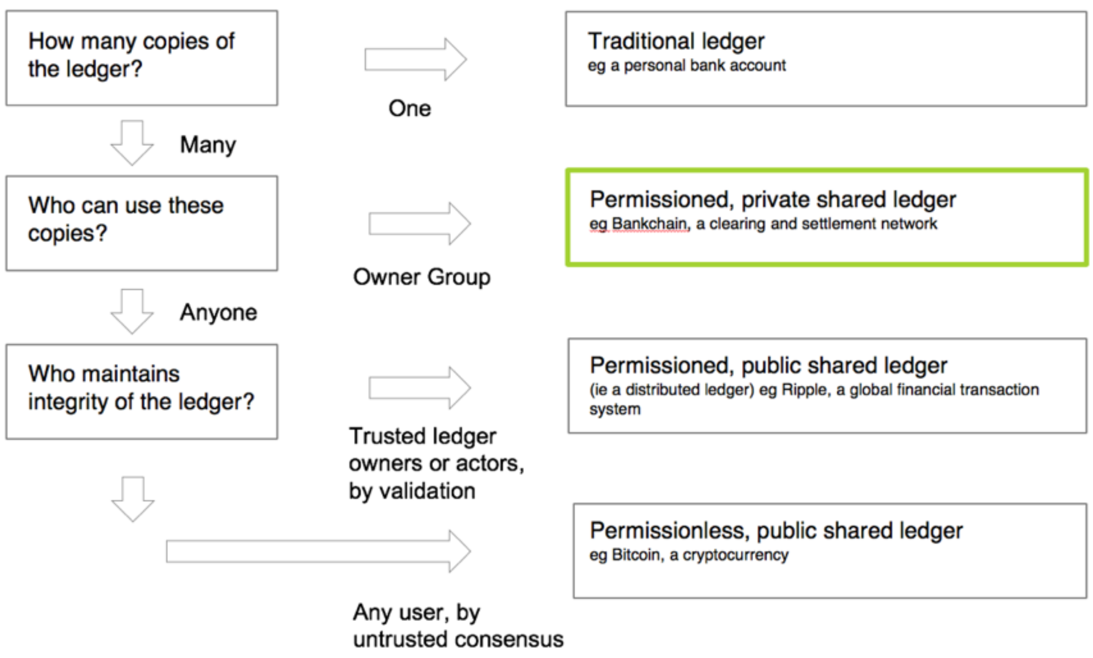
What is a DLT network?

A DLT Network is a network of computers, called network nodes, which implement a distributed ledger by running specialised software and communication protocols to share, synchronise and access the ledger records. When a ledger update happens, these nodes apply a consensus mechanism to agree on the ordering of transaction records and whether they should be included. The consensus mechanism allows the ledger to be tamper resistant and immutable and containing only confirmed and validated transactions. Because the nodes contain identical replicas of ledger records, users of nodes know that "What you see is what I see" when they access the ledger.

What is a permissioned DLT network?

The TAG DLT network is permissioned, as opposed to unpermissioned networks like Bitcoin that are open to anyone. It is pemissioned in three ways, (a) the participants need to agree to the governance and control principles to participate to the network, (b) the participants need to be approved to become network members, (c) the participants need to comply with the network minimum requirements at all times.

Ledger Taxonomy


How many copies of the ledger?
One
Traditional ledger
eg a personal bank account
Many
Who can use these copies?
Owner Group
Permissioned, private shared ledger
eg Bankchain, a clearing and settlement network
Anyone
Who maintains integrity of the ledger?
Trusted ledger owners or actors, by validation
Permissioned, public shared ledger
(ie a distributed ledger) eg Ripple, a global financial transaction system
Any user, by untrusted consensus
Permissionless, public shared ledger
eg Bitcoin, a cryptocurrency

Source: Dave Birch, Consult Hyperion

Why should trade associations set up a DLT network?

To resolve the industry's trust problem by enforcing measurable industry standards, certifications and legal requirements across the industry on an ongoing basis over an always-on decentralised industry wide network, supported by a DLT platform and operated in the best interest of the industry as a whole. This cannot be achieved with centralised solutions controlled by single entities.

Who defines the requirements and makes the decisions?

The network governance entity that is formed by trade bodies, and other industry representatives (this is to be further defined) as representatives of the industry as a whole.

Who operates the network?

As a trade body representing the entire industry, TAG is planned to act as the network operator under the supervision of the network governance entity.

How do the network requirements get enforced?

Requirements that are measurable over the data provided to the platform get enforced over the DLT platform. Requirements that are not measurable will go through a traditional audit process.

How does the network fight fraud?

Any company joining the network needs to comply with minimum requirements to become a network participant allowed to use the network. By providing access to information on the advertising delivery to be reconciled among supply chain participants, the detection of discrepancies between them is providing a signal for potential fraud. The company may lose this right and be prevented from participating to transactions should the ledger provide evidence that the company does not comply with network requirements at all times.

Who does get access to the data?

A consent framework will be activated as part of the network functionality. Depending on the case, access to data may require one or more parties to provide their consents. As all consents can be easily provided by all parties using the network's API or the Live Compliance user interface, this procedure won't be time consuming. Consents are automatically enforced within the network's infrastructure. The data provider remains in control of the access as he voluntarily can decide whether to report data or not.

Who can build applications?

Anyone in the industry can contribute to the development of the network application ecosystem using the platform API providing access to the distributed ledger.

Why should I participate?

The network provides accountability and compliance, while driving business value and efficiencies for network participants at a minimal cost compared to the benefits it generates.

What are the participant benefits relative to costs?

Based on a cost not to exceed 1% of the advertising spend, the cost/benefit ratio could reach a high multiple. The network provides a range of benefits in itself, that can be enhanced over system integrations and applications.

Is a DLT network adding a layer of complexity?

DLT is a breakthrough in various industries as a technology solution taking away the complexities and inefficiencies of supply chains by allowing to share and reconcile transaction data among trusted business partners in line with their contractual agreements in a secure and trusted collaborative environment. It most notably takes away the need for lots of different integrations between different organisations, it simplifies legal agreements among participants and allows to automate them over smart contracts, compliance information becomes readily available and always-on reporting contributes to the reduction of expensive reconciliation and auditing.

If I already get log files from other supply chain participants, why would I need this?

Building log file integrations with every partner in the ecosystem is expensive. Maintaining them when they are up and running is also expensive because it comes with a substantial commitment to keep technology up to date: partners will always change their technology, naming conventions, access settings or update specifications over time. With the TAG Network only one integration is required to get access to the logs of every other network member. Moreover, log file data can be downloaded already pre-reconciled according to defined rules and be used for automated business agreement management. For these reasons, we think that - for most companies - DLT will be a cheaper, more efficient way to get access to log files than other methods.

Does the industry need common log file standards if it has DLT?

Log files reconciliation requires for log file data provided by various individual supply chain participants to be consistent. One way to address this question is to define detailed standards for log file formats, data fields naming conventions, taxonomies and meanings. To come to an agreement on industry logging standards is likely to take time and will require significant investments from adtech vendors to adjust their logging systems.

Another approach is to write log files data to the DLT network, where it is automatically harmonised to a common network format at the moment it is written. This approach requires less investments from ad-tech vendors, as it allows to use any formats, taxonomies and naming conventions as long as they can be harmonised to a common format. The only standard required to avoid any ambiguity is to define the meaning of data fields. With this approach the log files reconciliation functionality may be supported by the industry much faster with minimal changes required from ad-tech vendors.

What is a smart contract?

A smart contract is a computer program stored in a distributed ledger network wherein the outcome of any execution of the program is recorded on the distributed ledger. A smart contract might represent terms in a contract in law and create a legally enforceable obligation under the legislation of an applicable jurisdiction. Smart contracts allow organisations to automate their business relationships using software code with enforceability based on the distributed ledger records.

What is the Reconciliation SDK?

The Reconciliation SDK (software development kit) is a tool developed by Fiducia that can be installed on publisher sites and applications. It creates a log file record ID map when an ad is requested that can then be shared with every supply chain participant. With this ID map, log files of various supply chain participants can be all matched deterministically line to line. The SDK is preserving consumer privacy and can't be used for consumer tracking.

Does the network create a new monopoly?

For the TAG DLT network to deliver all its benefits it has to be widely adopted across the industry as a "new standard" in the way to conduct business. This is the reason the network needs to be set-up *by the industry for the industry* as a consortium under an open governance that truly represents the whole industry. Rather than creating a monopoly, the network is helping to create a fair and open marketplace based on trust with the enforcement of self-defined rules that all participants across the supply chain agree to implement consistently at all times.

10. Glossary

API - An application programming interface (API) is a computing interface which defines interactions between multiple software intermediaries. It defines the kinds of calls or requests that can be made, how to make them, the data formats that should be used, the conventions to follow, etc. It can also provide extension mechanisms so that users can extend existing functionality in various ways and to varying degrees. An API can be entirely custom, specific to a component, or it can be designed based on an industry standard to ensure interoperability.

Blockchain - A blockchain is a type of distributed ledger, comprised of unchangeable, digitally recorded data in packages called blocks (rather like collating them on to a single sheet of paper). Each block is then 'chained' to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions.

Cryptographic key - A piece of information that determines the output of a cryptographic algorithm. Keys are usually used as a way to provide or gain access to a system or information.

Digital signature - A code attached to an electronically transmitted document to verify its contents authenticity and integrity.

Distributed ledger - A type of database, which stores transaction records and is consensually shared, synchronized and accessible across multiple organisations, sites, institutions, or geographies. A distributed ledger stands in contrast to a centralized database, which is more prone to failures, cyberattacks and fraud, as it is administered by a single organisation and therefore has a single point of failure.

Distributed Ledger Network (DLT Network) - A network of computing devices, also called distributed ledger network nodes, which implement a distributed ledger by running specialised software and communication protocols to share, synchronise and access the ledger records. When a ledger update happens, nodes apply consensus mechanism to agree on the transaction record inclusion and ordering. Consensus mechanism allows fulfilment of the distributed ledger design goals to be tamper resistant, append-only and immutable, containing confirmed and validated transactions. The fact that nodes are storing consensual replicas of the ledger records may be expressed as "What you see is what I see".

Distributed Ledger Technology (DLT) - Technology that enables the operation and use of distributed ledgers.

End-to-end Encryption - A system of communication where messages are encrypted and decrypted only by the communicating parties. As a result, they are the only ones who can read the messages. It prevents potential eavesdroppers - including telecom providers, Internet providers, and even the provider of the communication service – from being able to access the cryptographic keys and decrypt the conversation.

Immutability - Property wherein ledger records cannot be modified or removed once added to a distributed ledger. Where appropriate, immutability also presumes keeping intact the order of ledger records and the links between the ledger records.

Industry Consortium DLT Network - A DLT Network to store an industry marketplace transaction records, which is intended to be governed and operated by a consortium of industry organisations.

Log data - Data produced by a computing system that represents electronic records of the interactions with the system: for example, the record of an individual impression's sale or measurement. Usually captures an interaction type, content, time of the interaction and identifiers of the involved parties.

Scalability - A change in the size or scale to handle the network's demands. This word is used to refer to a project's ability to handle network traffic, future growth and capacity in its intended application.

Smart Contract - A computer program stored in a distributed ledger network wherein the outcome of any execution of the program is recorded on the distributed ledger. A smart contract might represent terms in a contract in law and create a legally enforceable obligation under the legislation of an applicable jurisdiction. Smart contracts allow organisations to automate their business relationships using software code with enforceability based on the distributed ledger records.

11. Reference Documents

Referenced Documents

- ISBA Programmatic supply chain transparency study, ISBA in association with AOP, carried out by PwC, May 2020. https://www.isba.org.uk/media/2424/executive-summary-programmatic-supply-chain-transparency-study.pdf

- Arresting the Decline of Public Trust in UK Advertising, Advertising Association, April 2019. https://www.adassoc.org.uk/wp-content/uploads/2019/03/AA_Public_Trust_Paper.pdf

- Online Platforms and Digital Advertising, Market study final report, CMA, July 2020. https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf

- Legal statement on cryptoassets and smart contracts, The LawTech Delivery Panel, UK Jurisdiction Taskforce, November 2019. https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf

- Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework, INRIA, February 2020. https://arxiv.org/pdf/1911.09964.pdf

- Governance Guidelines, Corda Network Foundation https://corda.network/governance/governance-guidelines/

Other Reference Documents

- 2nd Global Enterprise Blockchain Benchmarking Study, University of Cambridge, 2019. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-10-ccaf-second-global-enterprise-blockchain-report.pdf?v=1601044242

- Blockchain: 2020 Vision, Shaping enterprise blockchain adoption, R3 Corda, February 2020. https://www.r3.com/wp-content/uploads/2020/01/blockchain_2020_vision_shaping_enterprise_blockchain_adoption.pdf

- Blockchain Application in AdTech, IAB TechLab, Dec 2019. https://iabtechlab.com/wp-content/uploads/2019/12/Blockchain_Application_in_AdTech_IABTechLab_2019-12.pdf

- Blockchain Demystified, IAB Europe, April 2019. https://www.iabeurope.eu/wp-content/uploads/2019/04/IAB-Blockchain-Report-WEB.pdf

- Blockchain & Marketing, Technology Design Considerations for Implementation, GroupM, March 2019. https://www.groupm.com/groupm-blockchain-marketing/

- Corda Introductory White Paper, May 2018. https://www.corda.net/content/corda-platform-whitepaper.pdf

- Is blockchain the answer to digital advertising's trust gap?, PwC, 2019. https://www.pwc.com/us/en/industries/tmt/assets/2019-blockchain-in-advertising.pdf

- Deloitte's 2020 Global Blockchain Survey, Deloitte, 2020. https://www2.deloitte.com/content/dam/insights/us/articles/6608_2020-global-blockchain-survey/DI_CIR%202020%20global%20blockchain%20survey.pdf