Un-Blocking identity in a digital world

Using distributed ledger technology for customer due diligence

March 2018

A Whitechapel Think Tank discussion paper

UK FINANCE

As part of our ongoing work to engage with industry developments, UK Finance provided secretariat support for the Whitechapel Think Tank (WTT) on this report. The WTT is focused on technological innovation in financial services and is a forum to build an understanding of the opportunities and challenges presented by distributed ledger technologies (DLT). Open to stakeholders interested in the safe and efficient introduction of DLT, it is a neutral and transparent forum to explore this technology opportunity and provides a non-competitive environment to progress the advantages of the collaborative agenda. Membership includes industry, academia, regulators and the UK Government.

Contents

Foreword

Validated identity is a major requirement for doing business and transacting in the digital economy. It is vitally important to the financial services industry and the subject of detailed legislation and regulation. Business and personal customers prove daily who they are to transact and receive goods and services.

But the concept of identity is complex. Identities can be applied to different types of entity – individuals, organisations and assets. Identities can multifaceted, depending on the role or persona that is being undertaken at any given point in time: for example, an individual may be acting as a citizen, an employee or a customer. The nature and standard of proof that is required to establish and validate an entity's identity may also vary, depending on the service or benefit for which the proof is required. There are also various sources of data, drawn from both authoritative and corroborative sources, that can be used to satisfy that proof to the required standard.

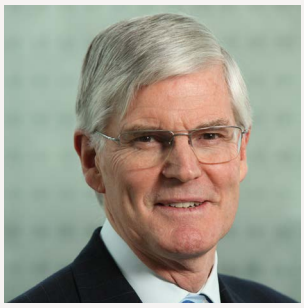
The digital economy holds out the prospect of vastly more efficient means of exchange, but it must be supported by a system for establishing and validating identities that is robust. For that reason, there is a wide-ranging debate about digital identity, public and commercial identity solutions and innovation in both the public sector and commercial market.

The Whitechapel Think Tank's purpose is to consider the application of advanced technology and, in particular distributed ledger technology (DLT) in the financial services industry. This report looks at how DLT could provide a solution to the "identity problem" – where current methods are costly to industry and the source of customer friction.

DLT enables a decentralised approach not only to sharing sources of data that are used to undertake a proof of identity, but also to fostering a market for the identity proofs that are created as a result.

DLT has the potential to address many issues – it leaves the data subject in control of their data, it allows proof of identity to be decentralised rather than maintained in a central authority, and it enables participants to commercialise the due diligence work that they already undertake to establish and validate identities.

This paper considers how DLT could be utilised to assist in streamlining the approach to proof of identity and verification. It is intended to provide a paper for discussion rather than to propose a conclusive solution to the challenges of customer due diligence in an increasingly digital economy.



Jeremy Wilson
Chair
Whitechapel Think Tank

Stephen Jones
Chief Executive
UK Finance

Executive Summary

Validated digital identity is a challenge for all digital service providers. Customer Due Diligence ("CDD") – i.e. how to be sufficiently certain of corporate, individual and SME identity and entitlement to be able to deliver a service – is particularly important for financial services and government, given the roles that they play in the economy. The Whitechapel Think Tank has examined the potential application of new technologies to solve this problem, with a focus on DLT.

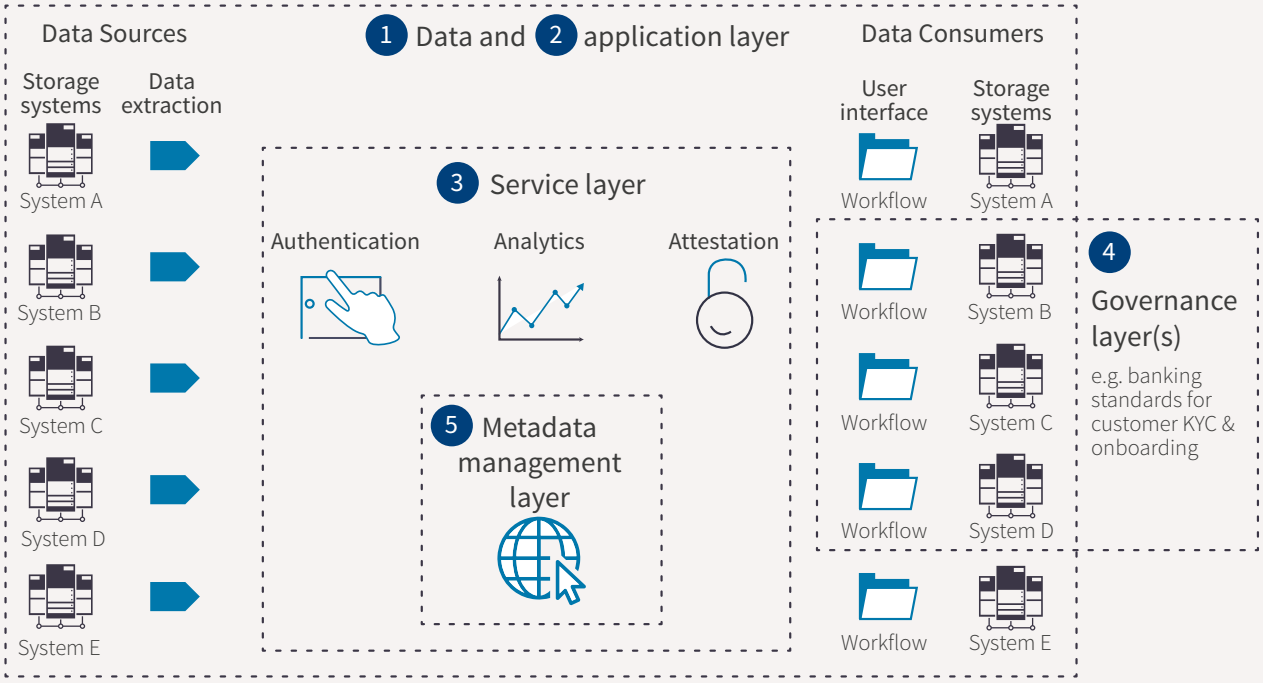
It is clear there needs to be a business case that is attractive to all participants if identity solutions are to develop at pace. Current authoritative (DVLA, Passport Office) and corroborative sources (banks) of identity are distinct and separate, operating to their own standards and governance. DLT has the potential to provide a unifying and enabling technology linking different sources. Used in the right way, an approach based on DLT can leave the data subject in control of their data, enable proof of identity to be decentralised rather than maintained in a central authority and allow participants to commercialise the work that they do to validate digital identity.

This paper first analyses what is meant by digital identity, its characteristics and its potential uses. It considers the common components of three use cases, suggesting some fundamental characteristics which form the basis of any technology application, including distributed ledger technologies, to validate identity. The three uses cases are:

- CDD for correspondent banks;
- account opening for SMEs; and
- access to government e-services for citizens.

Despite some headline differences between the use cases studied, our analysis suggests that there is a common framework that can be developed across the different scenarios. That framework has five layers: an application layer; a data layer; a service layer; a governance layer; and a metadata layer.

Figure 1: Framework for digital identify verification through a DLT platform



Within the framework, the use case analysis suggests that there are two potential approaches that would provide the technical base to enable institutions to undertake proof of identity in a way that is more efficient, effective and better suited to the digital world. The first is for all institutions within a specific context to rely upon a standardised proof of identity that is universally recognised[1] as being authoritative. The second approach would be for all institutions to use a standardised metadata management protocol to govern access to distributed data and distributed service providers[2] which they can then combine to meet the standards required by a multiplicity of different contexts.

DLT enables participants to be brought into a collaborative network. Those participants might include existing identity registers and authoritative data sources (such as the DVLA or the Passport Office), corroborative data sources (such as the banks and other service providers), service providers that undertake data verification and identity proofs to given standards (such as credit bureaux) and service provider applications that require such proofs in order to trade with confidence in the digital economy.

A DLT also creates the potential to share state of data records (i.e. metadata), meaning that all participants can be simultaneously made aware of the state of any record of identity proof, dis-proof or assertion (although the identity proof itself need not be held on the DLT).

The system could be open to all – known as permission-less – or accessed only by suitably qualified entities – known as permissioned. This means that it can be applied in either of the two approaches suggested by the use case analysis.

The Whitechapel Think Tank's contribution to the identity debate is to highlight the potential for DLT solutions to be considered. DLT could enable a decentralised approach to sharing both authoritative and corroborative sources of identity proof enabling both to be brought together in a collaborative network, where the transactions on the DLT provide further identity proof data integrity and origin.

In conclusion, this paper illustrates the potential application of DLT to the requirement for validated digital identity. The current processes are both costly and inefficient, unsuited to the needs of the digital economy. The rest of the paper examines these issues in more detail.

1 Appendix A describes this approach in more detail

2 Appendix B describes this approach in more detail

Identity

Identity, both personal and corporate, together with mechanisms for its assertion and authentication, is central to any modern economy. These mechanisms are needed – amongst other things – to qualify for a service or entitlement; to manage serious risks including economic crime, terrorist financing and fraud; to ensure that goods and services reach their intended recipient; and to ensure that payments are secure. While multiple mechanisms exist for the physical world solutions for the digital economy remain in their infancy.

It is therefore vital that an assertion of an identity made by an entity (whether individual, organisation or asset) can be trusted and safely authenticated. As modern economies are global and increasingly digital in nature, it is also vital that any identity solution is accepted broadly, scalable, and designed for a digital world.

The process of identity management involves many elements. An initial proof of identity is required to determine not only 'who are you?' but also 'do you qualify?' in the context of the service or entitlement on offer. Once a claimant's identity has been proven or verified, the service provider typically creates an account for the claimant, who must authenticate themselves using shared credentials to access the account thereafter. They can then use the account within the limits set by the service provider (i.e. each account is associated with an authorised scope of action).

Of these elements, proof of identity is the most burdensome to enact. The nature of the proof of identity that is required clearly varies according to the context in which the claim is being made: different services require different standards of proof and have different qualification criteria. The context affects both the nature and quantum of the information that needs to be provided by the asserting entity. Similarly, the relying party (i.e. the institution undertaking the proof) will apply more rigour in certain contexts than for others, depending on their assessment of the risks involved. For example, the level of proof of identity required to hire a car differs significantly from that required to open a bank account.

In many contexts, law and regulation requires that a specific level of customer due diligence takes place. In some contexts, an agreed standard defines the precise basis on which the proof is achieved. Usually, however, the institution undertaking the CDD is responsible for the way in which it undertakes the due diligence and verification balancing the legal, commercial and reputational risks against cost and user convenience.

Regulation

In certain industries, such as banking, institutions are required to undertake customer due diligence to a standard set by legislative and regulatory provisions. These provisions are clearly established at international, European and UK level. European Supervisory Authorities' guidelines and UK industry guidance, such as the Joint Money Laundering Steering Group, sets out some of the ways in which the provisions could be met.

At the heart of the provisions is the application of the risk based approach. Measures are taken by the institution to identify, assess, and understand the risks it faces and appropriate mitigation measures are taken by it in accordance with the level of risk. This means there is the absence of prescription and a tick box approach.

Whilst the risk based approach enables institutions to tailor their control environment, for example, so that it reflects size, product, customer, geographical footprint and risk, it means there can be a multitude of different and equally effective ways to identify and mitigate risk.

For example, an institution may identify and verify a customer through the adoption of one approach, such as accepting data from independent sources, whereas another institution may well do so through another approach, such as through other types and number of sources. In both instances, the identification and verification has been achieved and reflects the inherent flexibility in the risk based approach.

The problem

There is no single, definitive source of identity – the real world is simply too complex. Organisations and individuals play different roles in different contexts, and have relationships with each other that change through time. The data that describes them (and facilitates their interactions) can be diverse, contradictory and duplicative. The context in which an 'identity' is relied on can vary so much that no single source can ever be trusted and authoritative in every single context.

That is not to say that the identity providers (IDPs) that exist today do not provide a valuable service. Rather, that their service is only reliable in specific contexts. For example, an online merchant may rely on Google's identity service when opening an account for a new customer, but an online bank cannot. This is partly because a bank requires a different standard of proof than an online merchant, and partly because regulations do not allow an online bank transfer liability when relying on third party identity providers.

Reliance and Liability

Reliance and liability are difficult issues both separately and when combined. International, EU and UK level legal and regulatory provisions set out in clear terms that an institution can rely only on certain persons and in certain circumstances to carry out customer due diligence measures. Further, the same legal and regulatory provisions set out in clear terms that notwithstanding reliance on another person, the institution remains liable for any failure to apply customer due diligence measures. Reliance is a separate and distinct concept to verification.

Institutions carrying out customer due diligence measures will identify the person and verify the identification on the basis of documents or information in either case obtained from a reliable source which is independent of the person whose identity is being verified. For example, the Passport Office issues a citizen's passport and the DVLA issues a driving licence, which are used to verify a person.

Reliance, on the other hand, enables an institution to rely on the customer due diligence measures carried out by a third party (for example, a third party identifies and verifies the customer) if that third party is either subject to the UK money laundering legislative provisions or an equivalent regime. Further, the conditions that must be met when engaging reliance are prescriptive.

The third party must effectively provide the customer due diligence information it has obtained to the institution and it must enter into a written arrangement under which the third party agrees to immediately provide copies of the identification and verification data to the institutions on request and the third party retains the data for a certain time period. Further, even if an institution relies on a third party, the institution still remains liable for any failure to apply customer due diligence measures. A starting point for streamlining the verification process would be to make a wide range of authoritative data sources accessible to institutions.

Organisations and individuals must therefore repeatedly provide overlapping but different information to prove their identity in each context, and then manage different credentials with which to authenticate themselves.

The process of CDD is a burden on all parties, costing time and money. Information about organisations and individuals is invariably distributed, held in any number of different places, in any number of different ways, and it takes time to be collected by the claimant or relying party. Similarly, the institution undertaking the CDD must validate different elements of the claim with each

relevant authority – official company registries, passport offices, banks and so on.

Furthermore, the process is also less effective than it could be. Information is often shared bi-laterally between the two main parties to a particular transaction or relationship with limited or no reference to previous activity that may have taken place in other circumstances. This increases the potential for fraudulent activity. First, where the entity making the claim intermediates the data collection process. Second, where the institution undertaking the proof cannot see whether other parties have already ratified the information being presented by the claimant, or if they have called it into question.

The purpose of this paper

In this discussion paper, we consider how DLT might or might not be relevant as part of the solution set to this problem. To do so, the Whitechapel Think Tank first explored three specific use cases of identity that exemplify the problem outlined above:

- Customer Due Diligence (CDD) for correspondent banks
- Account opening for SMEs
- Access to government e-services for citizens

The intention of the analysis was to isolate the elements that were common to all three examples and that could be used to create a common framework for looking at the problem. What follows are the common components of all three, suggesting some fundamental characteristics which form the basis of any technology application, including distributed ledger technologies, to validate identity.

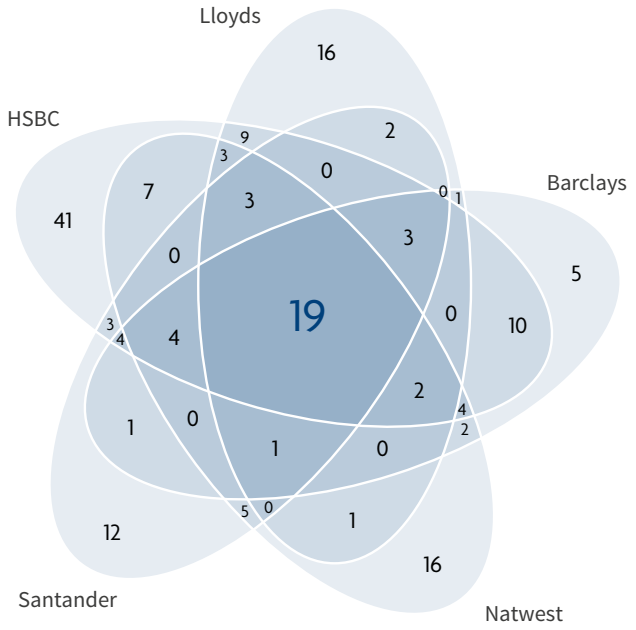
Use case analysis

Initially, the analysis reconfirmed the problem statement outlined above: namely, that the context for 'identity' varies significantly. This is perhaps self-evidently true across the three use cases, but further analysis showed that it can also be true within a particular use case.

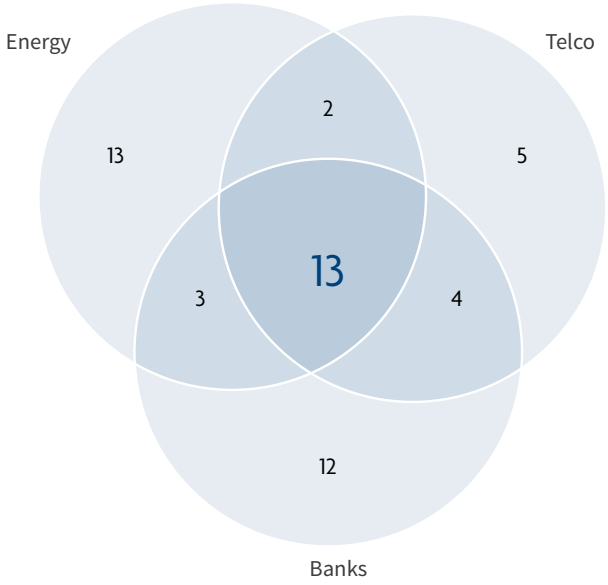
Figure 2: SME account opening (UK)

Example: SME account opening (UK)

Common questions by bank



Common questions by industry



The figure above shows how the data that is required to open an account for an SME in the UK varies not only by industry (right hand chart), but also by institution within an industry (left hand chart). This is, of course, because each institution is free to define their own SME onboarding process as part of a competitive market[3].

Heterogeneity across use cases is natural, because it reflects the complex reality of the different relationships that characterise our lives. Heterogeneity within a use case may also be desirable, if it promotes competition and innovation (for example, in assessing the risk associated with the SME looking to open an account).

The counterargument is of course that heterogeneity unnecessarily duplicates cost and effort, as both the entity making the claim (whether correspondent bank, SME or citizen) and the institutions acting as the relying party (whether correspondent bank, SME service provider or government e-service) undertake similar due diligence processes.

For example, for cases where enhanced CDD is required for correspondent banking relationships every correspondent bank is required to analyse each other's identity (i.e. it is a many-to-many relationship), even when they do business with each other regularly and consistently over time. Since each bank undertakes and maintains its own identity proof there is enormous duplication of effort across the system. The argument for standardisation in the CDD process for correspondent banks is strong. It is not a source of competitive advantage, but is a burden on all parties involved.

3 As part of the CMA remedies, UK Finance has delivered a common application form to make it easier for SMEs to open accounts ('Project Bulldog')

However, the analysis also showed that the case for standardisation is not always so strong. Relationships are not always many-to-many: sometimes they are one-to-many (for example, citizen to government e-services) and sometimes they are one-to-one (for example, an SME to its bank – although clearly there is a one-to-many relationship across industries). Equally, the cadence of work done varies: not every citizen accesses every e-service all of the time; SMEs do not switch service providers regularly, and are only required to revalidate their identity for regulated industries (like banking) every few years. Regulations also vary between jurisdictions and different requirements apply.

An initial conclusion of the work was therefore that standardisation of the CDD onboarding process is likely to be a solution in some but not every context.

Heterogeneity is sometimes necessary to reflect valuable differences across and within contexts, as in the case of an SME onboarding themselves to service providers from different industries, each of whom uses different qualification criteria. Even when heterogeneity is not strictly necessary (as in the case of SME bank account opening), the cost of converging existing processes may in fact outweigh the benefits of doing so for competing service providers.

Where heterogeneity is unnecessary and there is also a business case for the participating service providers, then convergence of standards can emerge as a result of market forces. In the absence of clear market incentives, the authorities (whether legislative or regulatory) may intervene to drive convergence of standards within a particular competitive space.

However, it is also clear that converging standards for identity proofing across all different contexts and for all different entity types (whether individuals, citizens, small businesses or large corporates) is challenging, and carries significant risk, as it would concentrate knowledge of nearly every aspect of our lives in a few authorities.

Common framework

Nonetheless, despite these headline differences between the use cases studied, the analysis did also suggest that there is a common framework or structure, comprising five separate layers.

Application layer

The application layer comprises the web-sites, mobile apps, processes and forms that collect, use and produce data about the entities that they engage with. The correspondent banks, SME service providers and government e-services are all operating applications and processes that need both to identify and qualify users (i.e. other correspondent banks, SMEs and citizens respectively) against context sensitive criteria.

As indicated by the figure above, it is the applications that specify the data they require to perform the identity proof and qualification exercise, as well as the process by which, and standards to which it must be undertaken. The results are relied on by the institution that operates the application and acts as service provider. And they are authoritative to that institution, as the latter is the ultimate owner of any decision that relies on the identity proof – for example, whether to deal with another correspondent bank, open an account for an SME or give a citizen access to government services.

While the applications themselves are inherently heterogeneous in nature, the existence of an application layer is common feature in the structure of all three of the use cases reviewed.

Data layer

Data sources hold the data that is required both to make the claim and to undertake the identity proof. Very often, the best data source is another application (for example, government e-services drawing on data about a citizen that is held by another government e-service).

Data sources can be authoritative where those sources are – by definition – the authors of the data (for example, a bank authors the bank account details of its SME customers; the passport office authors the citizenship of its citizens).

Data sources can be corroborative where data is being stored – and used – by third parties that are not the authors of the data (for example, a customer stores a delivery address with an online retailer; regular or recent use of that address to deliver goods corroborates its accuracy).

Access to private data sources about the claimant is, of course, carefully controlled. User authentication processes ensure that only the claimant, the subject of the data (and whose identity has already been proven to the data source), is able to share their data with the applications that need it.

As with the application layer, the data sources themselves, as well as the methods used to access those data sources, vary both across and within use cases. But it is also clear that all exercises in identity proofing need access to authoritative and corroborative data sources of some kind.

Service layer

The service layer comprises discrete elements of the identity proofing process, any one of which could be undertaken by a third-party service provider, such as data analysis and data verification or attestation.

Data analysis may include the collation, categorisation, combination, manipulation and assessment of data, such as the creation of a score of some kind or assessment against an agreed level of assurance. This may comprise the kind of service offered by credit reference agencies and others that may form part of the assessment of the claimant, be they a correspondent bank, SME or citizen.

Verification is the result of a due diligence process which involves a comparison of the data offered by an entity (a claim) with one or more authoritative or corroborating sources. Identity proofing is itself an exercise in verification, of course, but similar due diligence processes can be used to confirm the accuracy of the individual or multiple pieces of data, or of a particular attribute (such as the ownership structure of an SME), which form part of an identity proof.

While the range of these services is potentially very broad and many applications perform them internally, it is also clear that the proofing process can be broken down into individual process steps that can be undertaken by third party service providers. This service layer is common to the structure of all three use cases.

Governance layer

Some common standards exist across the application, data and service layers including are encryption standards that are used by data sources to store and transmit data (for example, ISO/IEC 18033-3 standard; authentication standards that are used to govern access to data (for example, the Strong Customer Authentication standards under PSD2); standards for risk assessment and analysis (for example, the Financial Action Taskforce ("FATF") and the EU Money Laundering Directive and Regulation); and standards for verification and attestation (for example, GPG 45 in the Gov. Verify scheme).

The governance model of each of the three use cases examined varied according to the extent to which common standards exist across the whole value chain of activity. The greater the convergence of standards, the more activity can be centralised or shared: for example, the UK government's Gov. Verify scheme gives citizens a single point of access to many (but not all) government e-services, but no such equivalent exists for SME access to commercial services because of the cost and difficulty of converging standards across such a heterogeneous population of actors.

Metadata layer

The final element that is common to the structure of each use case is metadata. Metadata is commonly referred to as "data about the data", but a broader definition would include "data about the data, the actors and their activities". This layer is largely implicit in at least two of the use cases examined, but nonetheless exists.

At the centre of the Gov. Verify scheme, for example, a hub maps the relationships between the citizen, government e-service and the citizen's identity provider. This hub is explicitly managing the metadata relevant to the Gov. Verify ecosystem, without viewing the data itself that flows between the different actors.

When an SME is onboarded onto a new service provider, they perform a similar 'hub' role themselves, as they are uniquely positioned to map the data requirements imposed by the service they are applying for with the data resources at their disposal, and they also navigate the user authentication steps required to share that data as part of their identity claim.

In contrast, most of the data required to fulfil correspondent banking CDD requirements is public. If sufficiently knowledgeable, an employee at the bank acting as relying party can therefore perform the hub role, finding and accessing the information needed, without needing to authenticate themselves to any of those sources.

Whether implicit or explicit, the metadata layer provides the detailed map that allows both the claimant and relying party both to map the relationships between different parties and to reference the data that are relevant to each specific context.

Potential solution sets

The use case analysis suggests that there are two potential approaches that would allow institutions to undertake proof of identity in a way that is more efficient, effective and better suited to the digital world.

The first is for all institutions to rely upon a standardised proof of identity that is universally recognised[4] within a specific context[5]. This can justify the centralisation of identity management into a single, authoritative source, so that individual institutions do not have to redesign their own applications to the same scope, using the same data, drawing on the same services or processes and working to the same governance models as others.

This approach is likely to be limited to a specific context or use case, such as KYC for correspondent banks, where the cost of convergence to a common standard (which is borne by the participating institutions) is justified by the benefits that it delivers in cost reduction and service improvement.

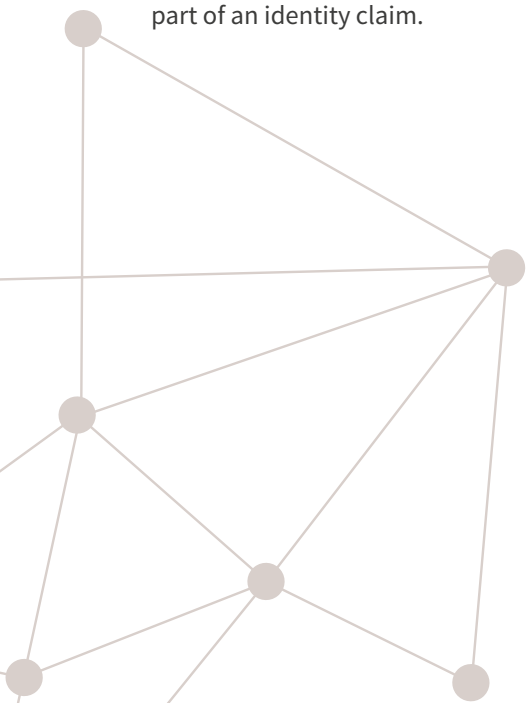
The second approach would be for all institutions to use a standardised metadata management layer that allows actors to navigate permissioned access to shared data and service layers[6]. This supports the aggregation of authoritative data sources and confirmation of corroborative data sources such that "trust" – i.e. the extent to which any relying party can use data as part of an identity proof – increases each time it is asserted as part of an identity claim.

This approach can be applied across different use cases, as it supports heterogeneity in the application and governance layers, and enables the re-use of authoritative data sources and value-adding services across those different use cases.

Others have of course looked at the identity problem. There is a number of publicly funded and commercial solutions that are already in the market, and several collaborative initiatives underway, each of which is seeking to address one aspect or another of the identity issue.

Of the two approaches outlined above, the first is by far the most intuitive, and the majority of the initiatives in the market place today are focused upon standardising proof of identity and subsequent user authentication for a particular context or use case.

Examples[7] include the Gov. Verify scheme for UK citizens, the Open Banking standards that apply to SMEs and the commercial utilities that support KYC for large corporates and financial institutions, such as those offered by Thomson Reuters, Accelus, SWIFT and others.



4 Appendix A describes this approach in more detail

5 For example, the TISA Digital ID

6 Appendix B describes this approach in more detail

7 Appendix C lists a number of public and private initiatives. The list is neither comprehensive nor definitive.

Fostering a marketplace

It is not the role of the Whitechapel Think Tank to evaluate or comment on this activity, other than to note that considerable efforts are being made and that potentially powerful solutions have begun to emerge.

However, if any of these identity solutions are to be more universally adopted, they must encourage participation. This means that there needs to be a business case that is attractive to all participants if identity solutions are to develop at pace.

The institutions which today control access to data are potentially powerful authoritative or corroborative data sources stores. To participate (i.e. share the data that they hold), they must benefit from providing third party access to that data, once it has been suitably permissioned by the customer. Since the data itself is owned by the customer, these institutions are best placed to benefit as providers of data services to other institutions, who act as relying parties. These services will include the analytical, confirmation or user authentication services outlined above.

The benefit case for the institutions acting as relying parties is easier to articulate, as they would get easier access to the data that their applications need to undertake a proof of identity. And they will benefit even more if they can place greater trust in that data. They are likely therefore to be willing buyers of confirmation services. They are also likely to be willing users of an explicit metadata layer, as they will place greater trust in the data they collate if they can not only see its provenance, but also how it is being used by other parties and liabilities managed.

The data subjects themselves must have a reason to adopt identity schemes either within or across different use cases or contexts. This will be driven by a combination of convenience and confidence. They are more likely to adopt an easy user journey which not only allows them greater control over their own identity and data, but is also useful to them in multiple different contexts including the ability to access new services and products. Regular and widespread use increases the utility of the scheme.

Supervisors, auditors and insurers must also have a transparent basis on which to assess risks and influence the behavioural norms of the market participants: data services such as identity proofing, user authentication and data validation involve the transfer of liabilities between institutions. This paper does not seek to solve for the issue of liability being transferred between institutions but recognises that this would need to be addressed regardless of the technological solution used to address digital identity.

More generally, regulators and government can fulfil their protective functions better by not only being involved in the setting of the rules by which each layer functions, but by assuring compliance with new and emergent regulation, such as GDPR.

It is both unlikely and perhaps unnecessary to replace existing centralised registers of identity validation records with decentralised versions. In many cases, what remains useful to be shared is the record of their existence and presentation to relying parties – the “metadata”.

Distributed Ledger Technology (DLT)

In completing customer due diligence checks, it is not always the specific actions taken by an institution that need to be recorded and shared, rather the record that there has been a successful (and current) CDD action by a recognised entity who has agreed to conform to a standard and whose assertion of CDD may be relied upon by a third party.

What characteristics does DLT have that would underpin a common infrastructure for identity management and providing a ubiquitous mechanism for assurance? There are four principal characteristics:

i. DLT enables these registers to be brought into a collaborative network. But also retain the benefits of a distributed proof of identity – rather than one all pervasive, central proof.

ii. The shared state of data records in a DLT means that all participants are simultaneously made aware of the state of any record of identity proof, disproof or assertion – there is no copying of the data causing delay, no central hackable honey pot of data and all views of relevant records will always be the same and unchangeable. This decentralised data management aspect of DLT addresses issues of distribution, copying and subversion to which alternative approaches may be subject.

iii. A specific action or set of instructions is always and every time performed in exactly the same way. Rules are commonly applied under all circumstances and therefore any participant can be certain that the results can be relied upon. This capability – of "smart contracts" – addresses issues in identity reliance of consistency across a network of relying parties and enables the development of services built upon identity records that automate agreed rules, further adding to the value the network and service provides to users.

iv. One of the major choices to be made in the design of any DLT is whether the system should be open to all – so-called permission less – or accessed only by suitably qualified entities – permissioned. The speed and cost of operating any DLT service is directly related to this choice; open or permission less systems require complex and expensive consensus mechanisms, closed or permissioned systems may not. We concluded that either may be needed depending on the ambition and scope of use of the service, and further that it is likely that different DLT approaches will be used for different communities of users and aspects of identity.

DLT and identity

The Whitechapel Think Tank believes that there are at least three potential models for the application of such technology in the identity space:

- **Secure data storage technology:** this approach could be used to create a common data layer on top of which different identity management schemes can be developed. The DLT solution would need to have embedded multi-party permissioning models as a core feature, so that ownership and privacy rights are respected.
- **Inclusion of standard identity proofs:** this approach would see the creation of standard identify proofs that could be stored on the ledger alongside the raw data itself. The provenance of the proofs (such as who authored them, the standard to which they were done and when they were undertaken) would be recorded as part of the transactional history on the ledger, which in turn would raise trust in their application by relying parties.
- **Using metadata:** a distributed ledger could be used to capture the metadata, which in turn could be read by participating institutions on a permissioned basis. The metadata would provide a basis for referencing and accessing the data and services needed to perform identity proofs, whether they were held on the ledger or not. This would then produce an evidential audit trail showing the use of and updates to digital identity over time, all of which would be recorded on the distributed ledger.

Conclusion

In this discussion paper, the Whitechapel Think Tank has shown the potential application of DLT to the requirement for validated digital identity. The current processes are both costly and inefficient, unsuited to the needs of the digital economy. As a result, there are a range of identity initiatives and solutions emerging. The WTT's contribution to the debate is to highlight the potential for DLT solutions.

DLT enables a decentralised approach to sharing both authoritative and corroborative sources of identity proof enabling both to be brought together in a collaborative network, where the transactions on the DLT provide further identity proof, with cryptographic assurance of data integrity and origin.

The authoritative and corroborative sources are currently distinct and separate operating to their own standards and governance. DLT provides a unifying and enabling technology – it leaves the data subject in control of their data, it allows proof of identity to be decentralised rather than maintained in a central authority and could enable participants to commercialise their validation of digital identity.

Appendix A – Corporate Authoritative

Today, the on-boarding of banks, by banks, involves every bank re-checking the identity checks done by every other bank. The costs tied to assessing identity are extremely high and the costs of getting it wrong are even higher. This repetitive and confused situation frustrates every banks' ability to evolve to meet new regulations and market changes, and exploit new opportunities.

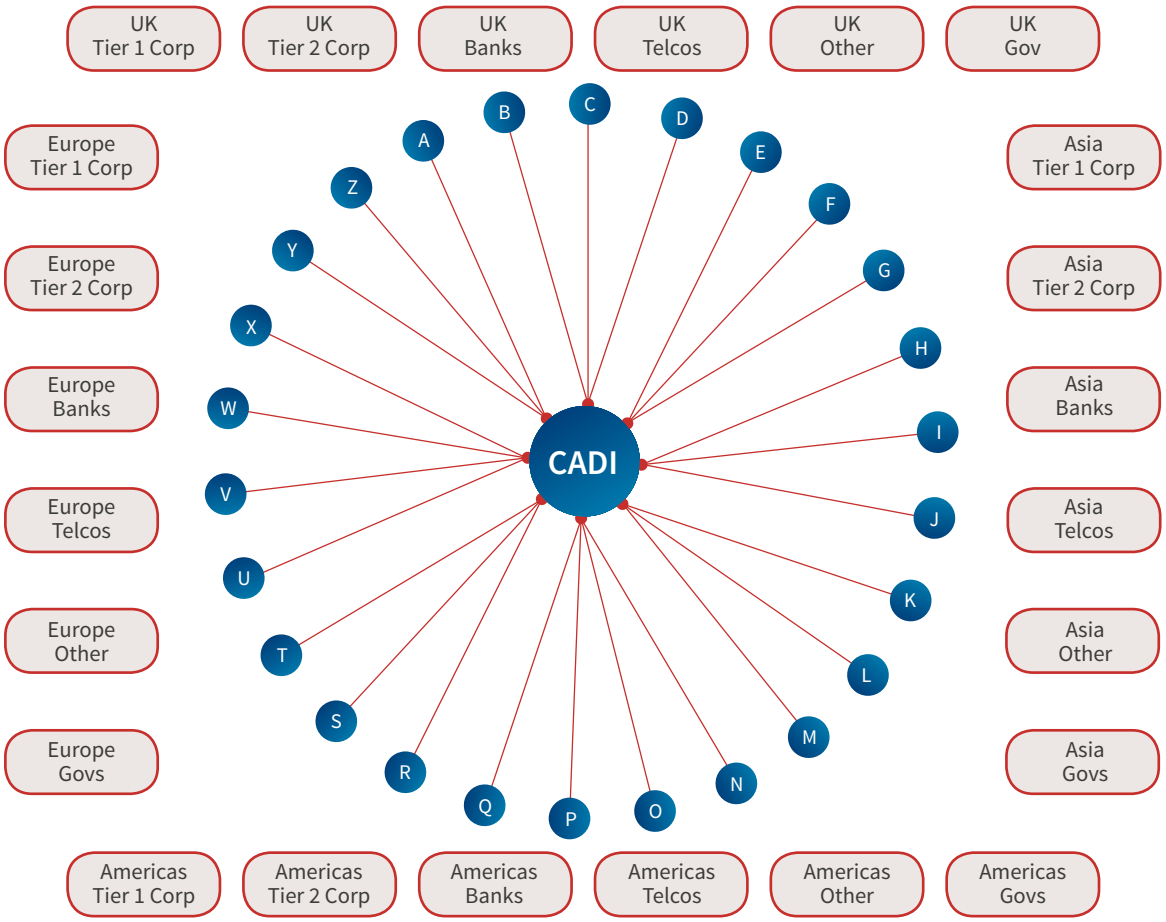
In the same way, the on-boarding process for all corporates is also duplicated by insurance companies, governments, and telcos. The same highly detailed and onerous on-boarding/Identity assessment is entirely decentralized, consumes enormous capital and human resources, lacks authoritative risk ratings, and leads to very different outcomes (for example enthusiastic on-boarding vs. de-risking, rejection or exit).

Great efficiencies and enhanced quality of output can be gained through a more collaborative approach to risk assessment. What appears to be clear at this stage is the need for more reliable, enhanced risk-based approach to analysis, coupled with multi-level interconnected risk assessment capability and 'authority' at country and international levels. Authoritative Digital Identity (ADI) refers to a proof of identity which is authoritative, digital and massively reusable, based on common policy and standards.

Distributed Ledger Technology (DLT) provides the means to assemble and store the authoritative data and analysis results, and provide an evidentially authoritative reference that is accessible throughout global financial systems, for business and risk management operations. DLT could enable this to become far faster and more accurately than is done today. Conversely, the use of DLT for business operations depends upon the existence of ADI to ensure consistency within and across all ledgers.

Together, ADI and DLT could result in an industry changing solution. This involves replacing the multiplicity of different, non-interoperable point-to-point links with a federated model where all financial institutions share the ability to access authoritative data under control. Potentially, this model could be extended to non-financial industry organisations and governments.

Figure 3:



This model would be delivered by adopting a federated model that leverages best practice models from other high assurance industries, international standards and independent assurance schemes. Requirements are:

i. Agreed standards around corporate CDD and onboarding OR agreed components of data

ii. Agreed ratings criteria for the varied levels of agreed standards

iii. Authoritative and corroborative sources of required data for identities

iv. Analysis of required data, based on standards

v. Assignment of a trusted, authoritative rating (or Level of Assurance) based on 1 through 4 above

vi. Accountability for the assessment and assigned rating, based on standards

vii. Technological compliance requirements, based on existing standards and regulations for trust

viii. Governance, including assurance and enforcement

ix. The legal policy framework

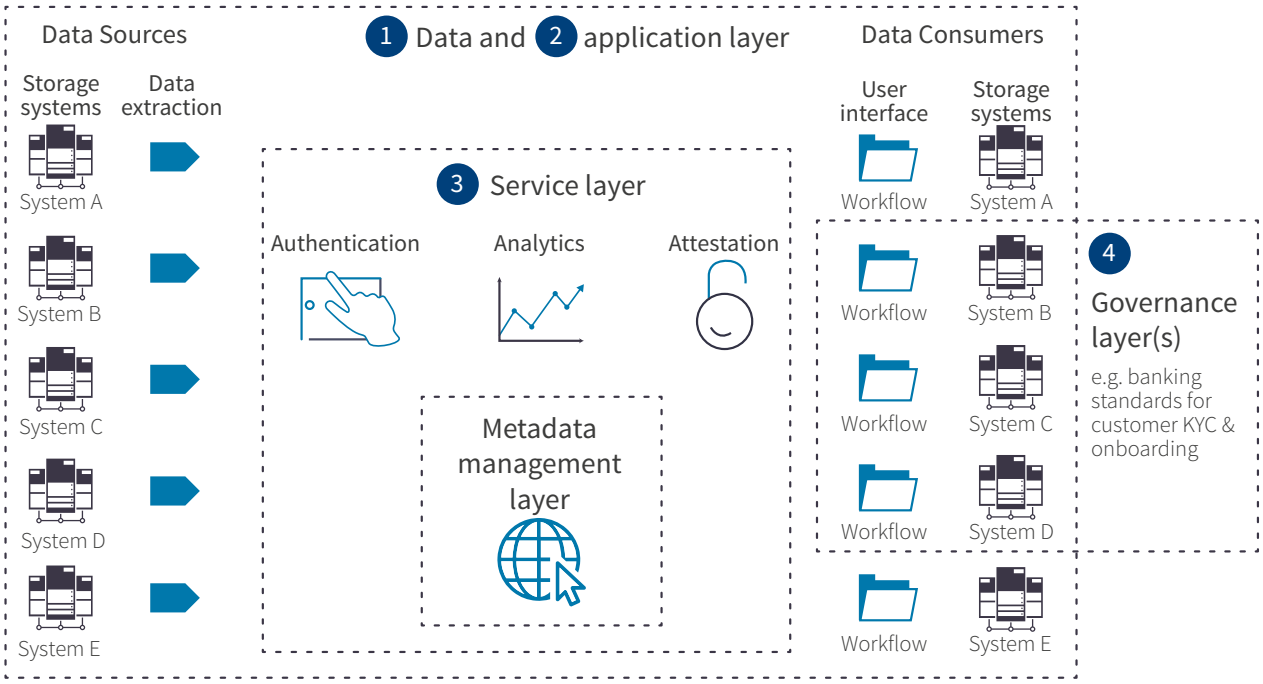
There is work underway regarding solutions for ADI which addresses the need for more efficient, higher quality assessments, and ratings for more efficient, informed on-boarding. The role of the WTT is to amplify the work already underway, identify the gaps and to accelerate the development of collaborative capabilities, such as CADI, to meet the demands of digital economies.

Appendix B – Metadata management layer

A permissioned distributed ledger could be used to create a common metadata management layer that governs access to data and services across a network of participating institutions.

An explicit and commonly used metadata management layer is currently absent from the overall identity eco-system – i.e. where metadata is recorded, it occurs within a specific context, and cannot be referenced or used outside of that context. This common layer would allow institutions to reference entities across different contexts, thereby building powerful beneficial network effects.

Figure 4: Framework for digital identify verification through a DLT platform



The solution would have the following characteristics:

i. The ledger holds meta-data only (i.e. it does not store values). An open-source protocol is used by applications to write to and read from the ledger.

ii. The protocol allows applications that act as relying parties to discover, and request access to, the data and services they need to engage with a given entity, regardless of where the data and services are held and the legal/regulatory rules governing its usage.

iii. In this design all access and usage is predicated on the suitable permissions being in place, which itself becomes an enforceable operation of the ledger. Permissioning models are designed to meet each context, ranging from the simple (e.g. consent from the data owner in a C2B context) to the more complex (e.g. the delegated authorities or multi-party authorisations that characterise B2B contexts)

iv. The protocol also allows applications acting as data stores to specify all the authorisations required to access the data they hold (including e.g. customer authentication) as their permissioning model, according to their own standards and governance model.

v. When all necessary authorisations are in place (e.g. consent from the entity, as data subject and data owner), the data can be routed to the requesting application. It is routed on a non-reliance basis.

vi. Trust in data quality is established through a combination of three effects:

vii. the application can call data from authoritative sources (i.e. sources that are trusted by the application);

viii. it can draw on network effects, visible in the meta-data, as an additional corroboration method;

ix. and it can buy data services (such as data analysis, verification, attribute confirmation, identity provision) from third parties which attest to data quality.

x. The latter assumes a competitive and innovative market for such services, also discoverable via the protocol. This market can be facilitated by smart contracts, executed on the blockchain.

xi. The proposed framework assumes that all applications are responsible for adopting practices which meet the requirements set both by the governance authorities that are relevant to them, and by any given standard that is necessary or desirable to adhere to. It does not force convergence.

xii. The proposed solution aims to facilitate strong data governance while minimising transitional costs and offering incentives to undertake the transition. By making meta-data management explicit, data stores codify the conditions that need to be met to access the data they host.

Appendix C – An overview of market initiatives

The principal initiatives are:

- UK Finance procedures for standardised SME account opening. Project Bulldog developed a common application form to make it easier for SMEs to open accounts.
- Project Factern is a data routing platform that enables SMEs to share their public and commercially sensitive data with counterparties in a controlled and structured format.
- UK Finance is taking forward Guidelines for Identity Verification. Authentication and Risk Assessment.
- PSF proposals being taken forward by UK Finance for Trusted KYC Data-sharing – a SME data sharing framework for sharing and storing SME data between banks. The proposed actions consist of establishing the necessary governance, defining standards, and specifying the mechanisms to establish a temporary testing environment.
- The Register of Legal Organisations (ROLO) registering organisational identity including for example, the unique property reference number fir the registered address, the Legal Entity Identifier, details of the Accountable Person, Directors and Trustees and Primary Beneficiaries and a wide range of other attributes.
- TISA is developing a digital passport for savers.

In addition:

- The Small Business Enterprise and Employment Act 2015 includes provisions that require designated banks to share credit data on their SME customers with credit reference agencies, who must then provide equal access to that data to finance providers.
- There is work underway to assess the potential to extend Gov.verify, which allows citizens to prove who they are online and access public services, for private sector purposes, including bank account opening .

There are also a range of commercial solutions in the market.