accenture

Position paper

SWIFT on distributed ledger technologies

Delivering an industry-standard platform through community collaboration

Contents

Executive Summary

Since the emergence of Blockchain and distributed ledger technologies (DLTs), the question of how this technology can be deployed in a business environment has captivated the industry. The search for implementations and use cases is now a key focus of R&D and innovation teams in major financial institutions, and is top of mind for executives seeking to determine future strategies for their transaction businesses and other data-driven operations.

As a financial industry cooperative, SWIFT's focus is on building technical, operational and business capabilities with a view to evolving our platform such that DLT-based services could be offered to our 11,000+ members, when the technology matures and firm business use cases emerge. Such DLT-based services could be provided by SWIFT, our community or third parties. In this context, we will continue to work with the financial industry to guarantee end-to-end automation and backward compatibility with legacy processes.

It is clear that industry-standard DLTs should be developed collaboratively with the industry in order to ensure the technology can be universally adopted. Drawing upon its long history of fostering industry collaboration, SWIFT will leverage its unique set of capabilities – unrivalled standards expertise and track record in security as well as our strong governance, operational efficiency, reliability and reach – to deliver a distinctive DLT platform offer for the benefit of its community.

This paper is the result of an in-depth assessment of the capabilities of existing DLTs carried out by SWIFT with the support of Accenture. Our analysis has confirmed that DLTs have the potential to bring new opportunities and efficiencies to the financial industry with their key strengths including the ability to create:

- Trust in a disseminated system;
- Efficiency in broadcasting information;
- Complete traceability of transactions;
- Simplified reconciliation; and
- High resiliency.

However, SWIFT's assessment has also demonstrated that, while some solutions have been successfully deployed in proofs of concept, existing DLTs are currently not mature enough to fulfil the requirements of the financial community. The following key requirements that DLTs need to attain in order to be widely adopted by the financial industry have been identified:

- Strong governance;
- Data controls;
- Compliance with regulatory requirements;
- Standardisation;
- Identity framework;
- Security and cyber defence;
- Reliability; and
- Scalability.

Our assessment concludes that significant further R&D work is required in each of these domains before DLTs can be applied at the scale required for the financial industry.

It is apparent that business standards will be key to the success of DLTs – it is always necessary to gain clarity and consensus about the meaning of shared data in a multi-party business environment, whatever the technology used. Existing standards, principally ISO 20022, will have an important role to play, both as sources of industry definitions and as enablers of interoperability between DLTs and existing automation technology, including financial messaging.

Equally, our assessment has highlighted that DLTs should not be viewed as a silver bullet to resolve all business issues; potential use cases should always be assessed to determine whether or not the key strengths of the technology could combine to resolve the business issue in question.

As part of its R&D programme, SWIFT is actively experimenting with DLTs and engaging with its community to identify areas in which they could bring concrete business benefits. We are developing proofs of concept in our SWIFT Innovation Labs spanning various ecosystems of available underlying technologies. As a Board Member of the Linux Foundation's Hyperledger Project, SWIFT is collaborating in an industry-wide effort to evolve open source Blockchain technology and build the foundation of a production grade distributed ledger implementation. In addition, through Innotribe, SWIFT's innovation initiative, we are forging collaboration between our members and FinTech companies. We will continue to engage with our community throughout our R&D process.

To find out more about SWIFT's work on distributed ledger technologies, please contact DLT@swift.com

Technology assessment of existing DLTs

SWIFT and Accenture have conducted an extensive assessment of existing DLTs in order to contrast the current technologies with the requirements that apply to any new solution to be adopted by the financial industry. Our multi-disciplinary team has examined the governance and compliance implications of the technology as well as technical aspects such as security, reliability, resilience, legacy integration and standardisation. The investigation has centred on operational matters and, as such, has not covered the legal implications of embracing DLTs. Moreover, our assessment is focused on inter-institution use cases, where SWIFT is providing services to the financial industry. It does not cover any potential DLT application within a financial institution, where SWIFT is not present.

Key strengths of DLTs

Our analysis has demonstrated that DLTs have the potential to bring new opportunities and efficiencies to the financial industry. The strengths of the technology include:

- **Information propagation** – Efficient means of keeping a full network up to date with latest information; distributed up-to-date ledgers allow the latest data to be updated and replicated in close to real time, ensuring all nodes are working from the same source of the truth.
- **Full traceability** – Participants or warranted trusted third-parties such as regulators are able to trace information flows back through the entire chain. Entries can be added to, but not deleted from, the distributed ledger, making ledger information immutable. This information potentially includes, but is not limited to, ownership, transaction history, and data lineage of information stored on the shared ledger.
- **Simplified reconciliation** – Local access to complete and verified data could ease reconciliation processes; since information is mutualised and all participants are working from the same data set in real time or near-real time. Current reconciliation processes, which suffer from latency and require significant human intervention, could be optimised and perhaps eliminated altogether.
- **Trusted disseminated system** – Participants are able to trust the authenticity of the data on the ledger without recourse to a central body. Transactions are digitally signed; the maintenance and validation of the distributed ledger is performed by a network of communicating nodes running dedicated software which replicate the ledger amongst the participants in a peer-to-peer network, guaranteeing the ledger's integrity.
- **High resiliency** – Operates seamlessly and removes dependency on a central infrastructure for service availability. Distributed processing allows participants to seamlessly operate in case of failure of any participants. Data on the ledger is pervasive and persistent, creating a reliable distributed storage so that transaction data can be recovered from the distributed ledger in case of local system failure, allowing the system to have very strong built-in data resiliency.

Technology assessment of existing DLTs

Applying DLTs in the financial services industry

Clearly, DLTs have the capacity to open up considerable opportunities for the financial industry. However, DLTs emerged from the consumer-to-consumer (C2C) market with the exchange of cryptocurrencies as a decentralised method of value transfer without third-party intermediaries. Evidently, the wider financial industry has an altogether different set of requirements than the application of individual consumers seeking alternative methods of value transfer. As part of our technology assessment, we have identified the following key requirements that DLTs need to attain in order to be widely adopted in the financial industry:

- **Strong governance** – Governance models to clearly define the roles and responsibilities of the various parties as well as the business and technical operating rules;
- **Data Controls** – Controlled data access and availability to preserve data confidentiality;
- **Compliance with regulatory requirements** – The ability to comply with regulatory requirements (e.g. Sanctions, KYC, etc.);
- **Standardisation** – Standardisation at all levels to guarantee straight-through processing (STP), interoperability and backward compatibility;
- **Identity framework** – The ability to identify parties involved to ensure accountability and non-repudiation of financial transactions;
- **Security and cyber defence** – The ability to detect, prevent and resist cyber-attacks which are growing in number and sophistication;
- **Reliability** – Readiness to support mission-critical financial services;
- **Scalability** – Readiness to scale to support services which process hundreds or thousands of transactions per second.

In the following sections we detail these requirements, set out the current maturity of DLTs in each of these domains, and identify the future research & development needed to bridge the gap between the capabilities of existing DLTs and the industry's requirements. Subsequently, we present the conclusions of our technology assessment.

Industry requirement

The services used by the financial industry need to rely on strong governance models, clearly defining the roles and responsibilities of the various parties involved as well as the business and technical operating rules supporting a particular business service. Strong governance is key to ensuring the delivery of effective, predictable and sustainable financial services.

Current maturity of DLTs

DLTs emerged through cryptocurrencies and use a community self-governing model, and, while it may be seen as fairly effective in that context, we believe that it does not provide the level of trust, transparency and accountability required by the financial industry. We have identified several governance issues. It is a fully open model under which anybody can join to submit and view transactions (i.e. a 'permissionless ledger'). While this may be a desirable characteristic in a consumer-to-consumer context, we are in favour of models in which only duly authorised participants can access the service and assess whether or not the interactions between participants are done in line with business pre-agreements and technical enforcement by the ledger. While 'permissioned ledgers' are a step in that direction, there is still work needed in order to provide the level of granularity – in terms of role profile definitions – required for the access control and participant interaction. Existing implementations of permissioned ledgers remain basic, only providing support for generic read/write profiles, the 'tokenisation of assets', and limited validation methods.

Future R&D

For applications in financial services, there is much debate over the role of a 'centralised' authority, creating and administering distributed ledgers with defined business rules versus open-source, or consortium-based models. While the former offers a stronger governance structure to reassure participants, it can also be perceived as limiting functionality and negating some of the benefits of DLTs versus the consortium model. The role of centralised governance versus open-source models needs to be investigated further, especially in the context of regulatory requirements and reporting, in order to ascertain the appropriate level of governance required.

Industry requirement

Data exchange in financial transactions is, in most cases, confidential. This is either because transactions contain personal data such as beneficiary details (and are therefore subject to specific laws governing the management of personal data) or because they contain information which could be used to derive competitively sensitive information regarding the activities of the parties involved. Data confidentiality is therefore a key requirement for any solution supported by the financial industry, and strong controls must be put in place to ensure that only duly authorised parties have exclusive access to the data relevant to them.

Current maturity of DLTs

Data on the ledger is held by all DLT participants with data broadcast between all parties. Although the identity of the parties involved in a transaction is theoretically hidden, thanks to the usage of an anonymous address instead of individuals or company names, this anonymity faces potential challenges in a business-to-business context. Here all participants will need to know the "anonymous" address of their business counterparties allowing addresses to be rapidly linked to the individuals or company concerned, giving full transparency and visibility on the ledger content.

Solutions to this problem are being investigated from a number of angles, but work is required to have a solution in line with the core confidentiality requirement. Encryption of the data is the typical solution used to address this problem, but one must be aware of the following considerations:

- It can be an operational challenge to manage encryption/decryption keys when there are multiple parties required to have access to the data as keys are required for each combination of parties involved. When more than two parties are involved, it can quickly become impractical.
- Data encryption may prevent verification of transactions as the transaction content may be hidden to the point where the network is unable to validate transactions or broadcast information to the ledger.

Future R&D

Work is required to better define what kind of data must reside in the ledger and should be distributed between participants. Alternative models should be investigated which are capable of distributing data sets only between the participants of a given transaction, either through peer-to-peer communication or another solution capable of truly guaranteeing privacy.

An interesting solution to the data privacy issue currently being explored is Zero-Knowledge-Proof (ZKP) algorithms which aim to allow the verification of content without having any knowledge of transaction content.

Industry requirement

The financial industry is heavily regulated and regulatory pressure is only increasing. Any solution must ensure that financial institutions are able to comply with their regulatory requirements and enable operations such as transactions and customer filtering against sanctioned lists, KYC, etc., while, at the same time, striking the appropriate balance between privacy and transparency.

Current maturity of DLTs

DLT compliance with regulatory requirements remains, to a great extent, unexplored and considerable work is still required. Key questions such as who should be regulated, and by whom, are yet to be answered with the answer far from straightforward due to the decentralised and cross-border nature of distributed ledgers. Moreover, it is not yet clear whether existing regulations need to be adapted for distributed ledgers, or whether new regulation will need to be created. Two schools of thought are at play here: either we continue to work within the current regulatory constructs (messaging, roles, process, etc.) or we disintermediate and change all of the above. The former option would be much more straightforward in gaining regulatory approval. This is certainly an area to watch, since regulatory attention heightens as interest in the technology grows and production use cases start to emerge.

Future R&D

R&D related to regulatory compliance in a distributed ledger environment will need to come from both the industry and regulatory bodies:

- Industry participants will need to clearly understand how DLTs will impact their ability to comply with regulatory reporting and audit requirements. Another area to consider will be the level of data granularity to be reported versus current regulatory mandates and how to provide appropriate levels of data detail without violating privacy laws.
- Regulators will not mandate how the industry explores, develops, and considers options to DLT solutions, but instead will respond to initiatives from financial services providers. To this end, there have been very positive comments recently from a number of regulatory authorities. For example, the US Commodity Futures Trading Commission (CFTC) recently encouraged distributed ledger exploration, warning regulators not to stifle innovation. Indeed, regulators have started to explore how DLTs will impact the way they operate as this impacts on their technology requirements as well as the skill set of their workforces.

Industry requirement

Standardisation is essential to ensure straight-through processing and interoperability between systems and participants as well as the correct interpretation of data being exchanged. In order to guarantee this, today's financial industry relies heavily on standards organisations such as ISO, ISDA (responsible for FpML), FPL (responsible for FIX), etc.

Current maturity of DLTs

Today's distributed ledger landscape lacks standardisation at all levels – from technical protocols to ledger and transaction data formats, to smart contracts. Moreover, distributed ledger development is being completed entirely in isolation from existing business standards organisations such as ISO, ISDA or FPL. The direct consequence of this lack of standardisation is that the various distributed ledgers are not interoperable and information stored on the ledger is not aligned to market standards and practices. Integrating a distributed ledger environment with a legacy system, if at all possible, may require extensive conversion and data enrichment.

Most discussions around standardisation of DLTs and smart contracts have focused on technical protocols and much work remains to be completed. As this work matures we can expect attention to quickly turn to business use cases and business automation standards. Compliance with business market practices will be required and, in order to ensure backward compatibility with existing legacy applications, DLT solutions will need to integrate into the wider transaction automation landscape which is rapidly evolving towards ISO 20022.

Future R&D

There are a set of fundamental questions to be addressed regarding standardisation:

- Is standardisation across distributed ledgers required or should DLTs have differing standards that are fully interoperable with each other and with those currently used in the industry? Requirements will need to be created as to how data/transactions can be passed between those solutions in order to optimise payment clearing speed, cost and reach.
- How can existing messaging and reference data standards such as ISO 20022 be best re-used in a DLT context?
- There will be a period of time when some financial services providers will have the ability to clear and settle transactions in a DLT environment, while others, who have not yet adopted the technology, will continue to transact on legacy infrastructure. Such a situation would potentially create a bifurcated market, distorting prices based on varying settlement times. Interoperability between these environments will need to be addressed both from an operational and regulatory perspective.
- Usage of smart contracts remains a key question in financial services owing to the nature of embedding business logic of a financial asset on the distributed ledger to be automatically executed. This is a very powerful concept and there are a number of potential use cases. Yet the need to understand what happens 'when it goes wrong', how to handle related errors and exceptions, the legal authority of smart versus traditional contracts, as well the standardisation of smart contract language, all will require serious time and effort on the part of financial services.

As mentioned above, to date DLT development has occurred in complete isolation from the current standards which drive efficiency across financial services. This creates potential challenges around integrating current operational processes, aligning assets that transact both in the current and future DLT environment, and in ultimately decommissioning legacy systems.

Industry requirement

A very strong identity framework is required to guarantee the identity of the parties involved in a particular business service, and to support non-repudiation of activities performed by the various participants. This is essential to provide trust in the system, ensure accountability and support any claims process. It is also a pre-requisite to be able to perform Know-Your-Customer and compliance checks.

Current maturity of DLTs

Linked to data privacy is the question of managing identities. In some existing distributed ledger implementations, participants remain pseudo-anonymous – a status not permitted to regulated businesses. The identities of both the participant organisation and those employees instructing the transactions will need to be traceable in a controlled fashion, that is to say, only by those who should have access. Indeed, following the 2008 crisis, the financial industry has invested heavily in legal entity identifiers and this needs to be an integral part of any solution.

Moreover, the key management system employed by DLTs to identify parties relies on self-signed keys supported by no recovery or revocation mechanism. This has the following implications:

- A key cannot be linked with certainty to an identity as there is no neutral third party certifying and guaranteeing that a particular key is associated with a particular individual or company.
- There is no facility to recover keys should they be lost, leading to assets being locked forever on the ledger should the ledger be used to track asset ownership.
- There is no facility to revoke a key should it be stolen or compromised. There is no way to indicate to other participants that a certain key should no longer be trusted and accepted by the system.

Future R&D

The question of key management, both in terms of issuance/identity and recovery, will require close examination. In the current proposed environment, one option would be to use a central certification authority (CA) maintaining a certificate revocation list and providing key recovery facilities. This certification authority would need to be operated by a neutral trusted third party. Such solutions are widely used by financial institutions, supported by existing infrastructures and processes, compliant with security industry standards such as FIPS level 2 or 3 and have a proven track record in terms of performance, security and operability. Leveraging this existing framework to address identity requirements is a natural solution, but further R&D work is required to demonstrate that when applied to DLTs they remain fit for purpose.

Industry requirement

Cyber-crime is a very real and ever increasing threat for the financial industry. Any DLT solution must be designed with the assumption that it will be subject to cyber-attacks, and thus must be able to detect such attacks and protect itself; moreover, with attacks growing in number and sophistication, cyber defence mechanisms must continuously be assessed, tested and improved.

Current maturity of DLTs

Originally, DLTs were designed as open systems, yet robust against cyber-threats, thanks to fault-tolerant algorithms performing transaction validation and ledger updates. These have been designed with the underlying assumption that a number of participants are malicious. Security is ensured through industry-standard cryptographic algorithms which are used widely across the industry. However, this high level of cyber resistance and security comes at a cost. Indeed, open distributed ledgers typically rely on a Proof-of-Work algorithm guaranteeing a high security level by ensuring that any ledger update has been done by a participant who has spent extensive computer resources in solving a cryptographic problem. Attacking the system would therefore require such computer power and resources as to render it not economically viable.

This model cannot, however, be translated to the financial industry: the cost would outweigh all the benefits. Hence alternative ways of securing the system must be examined, not to mention the scalability and latency issues. The industry trend is to rely on a private and permissioned ledger whereby participant access is strictly controlled and reliant on alternative consensus algorithms to perform transaction validation. Combined with the access control mechanisms, these algorithms aim at ensuring a similar level of protection whilst offering faster throughput and requiring far less computer resources.

Future R&D

As the ledger is distributed amongst participants, the protection of the non-encrypted data is left to the responsibility of each participant. This significantly increases the risk of data leakage even in the case of a private ledger where ledger access is controlled. To address this risk, more work is required to allow for partial or complete data protection on the ledger through the use of encryption or selective distribution.

The industry needs more R&D to understand the impact of the following:

- How does the cyber threat matrix change in a distributed ledger environment?
- Does removing the single point of failure create multiple points of entry?
- Could an attacker create denial of service by bombarding the network with false transactions in order to slow or even spread confusion in the system?
- The question of attack prevention and detection in a distributed environment;
- Whether, and how, a node can be isolated to protect the system;
- In a permissioned environment, who is going to ensure malicious actors do not gain access to the system either through hacking or bypassing KYC provisions to create new nodes?

Industry requirement

Certain financial services are crucial in guaranteeing the financial stability of the global economy and hence need to operate with the highest level of service. The ability to support mission-critical applications, such as RTGS systems or CSDs, requires enterprise solutions engineered to guarantee extremely high availability and the means to be able to recover from catastrophic failure scenarios.

99,999%

Current maturity of DLTs

Distributed systems are resilient constructs by nature and have a very strong ability to recover from failures without any loss of data. However, centralised systems already achieve record high-level service availability, with availability levels above 99% now common.

With no central infrastructure, service availability in a distributed system will depend on the availability of its participants' infrastructures, and therefore cannot be directly controlled by a central administrator. The obligation of availability therefore shifts to the participants of the distributed system and controls will need to be put in place to ensure that each participant meets pre-defined availability levels. This can only be achieved through very strict software development, qualification and release management as all software updates need to be applied by each participant. For example, weak cryptocurrency release qualification management cycles have already caused numerous issues, with emergency fixes required to recover from ledger inconsistencies (so called 'forks') resulting in interoperability and backward compatibility issues. This contrasts with a centralised system where an administrator can shield participants from a proportion of software upgrades which are applied only centrally.

In addition, the reliability of distributed systems has known limits. There is a maximum proportion of fraudulent participants that can be handled without compromising the integrity of a distributed system. Also, in the event of a network communication problem, distributed systems are susceptible to division, resulting in two or more groups of participants operating independently of each other (so-called 'partitions'). In such a situation, there is a maximum proportion of participants that can be isolated beyond which the system will not be able to restore a consistent ledger when the communication issue is resolved. Thus, the reliability limits of distributed systems need to be stated in clear service levels, understandable by business users in order that they are aware of, and can assess the business risks should these limits be exceeded and can also define the related business continuity plans.

Future R&D

To make a DLT-based solution fully reliable over multiple years or decades, R&D work still needs to be completed to define the right software management and release policy principles in distributed environment, in line with best practice of the industry such as ITIL.

Additionally, some operational aspects need to be examined considering the systemic risks that failure of a critical financial system can represent. This encompasses areas such as: how to enforce regular mandatory software upgrades, and apply emergency fixes to address bugs or security breaches; how to exclude non-compliant nodes; how to inform participants should they become isolated; and how to ensure data recovery from the ledger in case a local issue is fast enough to resume business operations as per defined service level agreements.

Industry requirement

It is not unusual for systems in the financial industry to support throughput in the order of several hundreds or even thousands of transactions per second. Therefore, any DLT solution to be used by the financial industry must be guaranteed to cope with the scale of the use case it is addressing.

Current maturity of DLTs

As a consequence of the 'Proof of Work' algorithm used by distributed ledger implementations deriving from Blockchain, those implementations are limited to a fairly modest number of transactions per second (TPS). This algorithm also introduces the possibility for the ledger to 'fork' into multiple ledger versions held by different participants, and, while forks are automatically corrected statistically after a few ledger updates, the whole process is lengthy with transaction "finality" reached after a considerable period of time (e.g., close to an hour in the case of some cryptocurrencies).

Using alternative consensus algorithms, described above, allows both problems to be solved. A number of current solution providers are experimenting with very high TPS and some have shown great promise. Such numbers should be treated with caution, however, as they have yet to be demonstrated in production-like environments with hundreds of participants geographically dispersed around the world submitting transactions simultaneously, which could significantly impact both the achievable throughput and the transaction latency. This is nonetheless a very encouraging and promising development which should be able to cater for a very large number of applications – although it may not be robust and scalable enough for extremely high throughputs and very low latency systems, such as those employed by trading platforms to support high frequency trading (HFT). Inherent to the concept of the distributed ledger is the fact that the information is stored forever. This may bring significant challenges from both a storage and network bandwidth point of view, as the volume of transactions increases.

Future R&D

R&D needs to be carried out in order to assess the various available consensus algorithms and validation methods against realistic and representative business throughput requirements. As such, tests need to be conducted in production conditions rather than lab environments to assess the robustness of the algorithms in exception scenarios and under stress. In particular, the following activities need to be conducted:

- Validation of the various systems against the CAP theorem ruling distributed systems in order to understand the practical limits beyond which consistency, availability and partition tolerance can no longer be guaranteed as well as how to recover in case such situations arise.
- Simulation of DLT behaviour in a WAN environment, prone to network disruption and where network latency between various participants can vary significantly based on physical location and available connectivity.

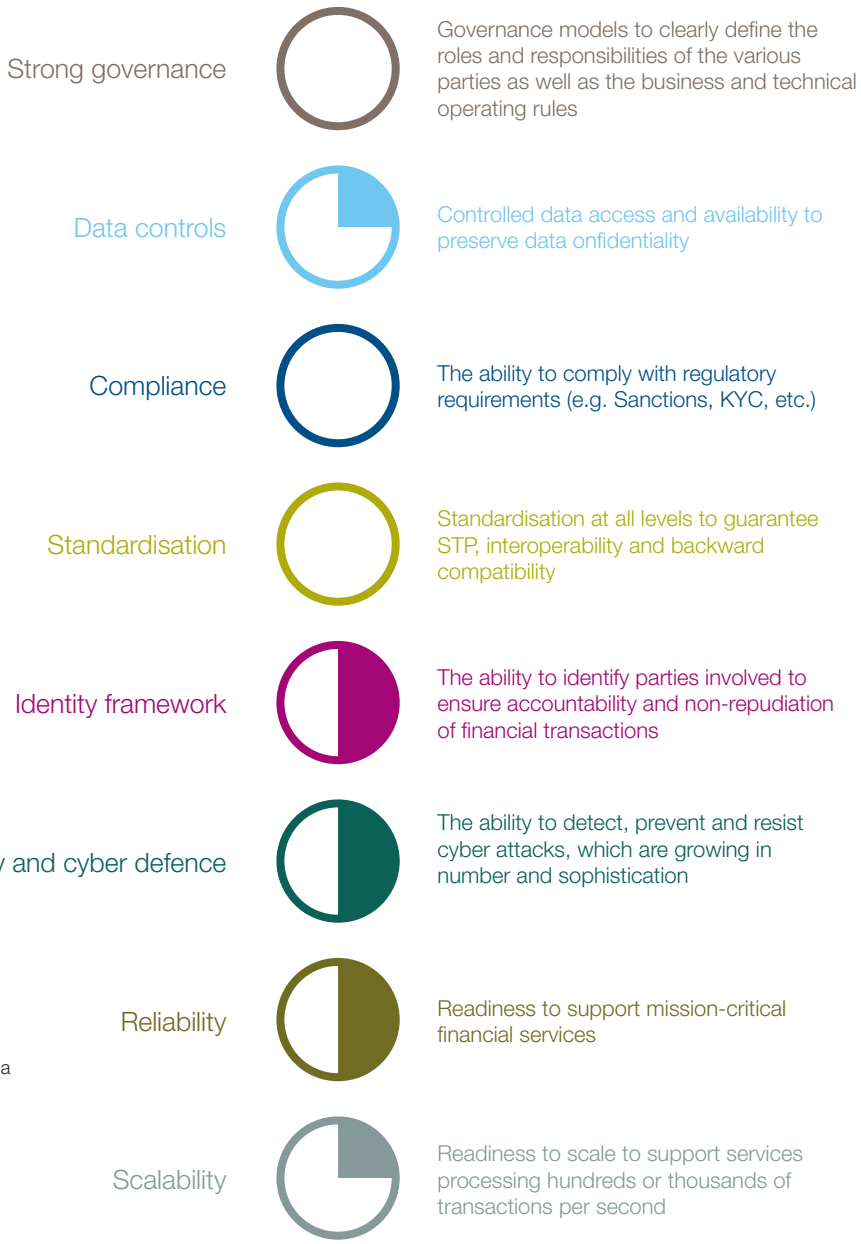
Conclusions of the technology assessment

As summarised in the following graphic, our assessment has demonstrated that, while there are promising developments in each of these requirements, significant extra R&D work is needed in all these domains before DLT can be applied at the scale required by the financial industry. Despite the emergence of new solution providers, and the natural maturation of existing software, there is no single mature DLT solution yet on the market that addresses all the requirements necessary for an enterprise grade implementation, with many questions remaining unanswered. As such, DLTs are at an early stage in their development. Further research, development and testing is needed to fully understand the capabilities of the technology and the business use cases best suited to it.

Moreover, additional research needs to be conducted regarding: the interoperability of DLT systems with legacy infrastructure; the interoperability between distributed ledgers across multiple counterparties, and the regulatory requirements to do so; as well as standardisation.

Equally, our assessment has highlighted that DLTs should not be viewed as a silver bullet to resolve all business issues; potential use cases should always be assessed to determine whether or not the key strengths of the technology could combine to resolve the business issue in question.

Maturity assessment

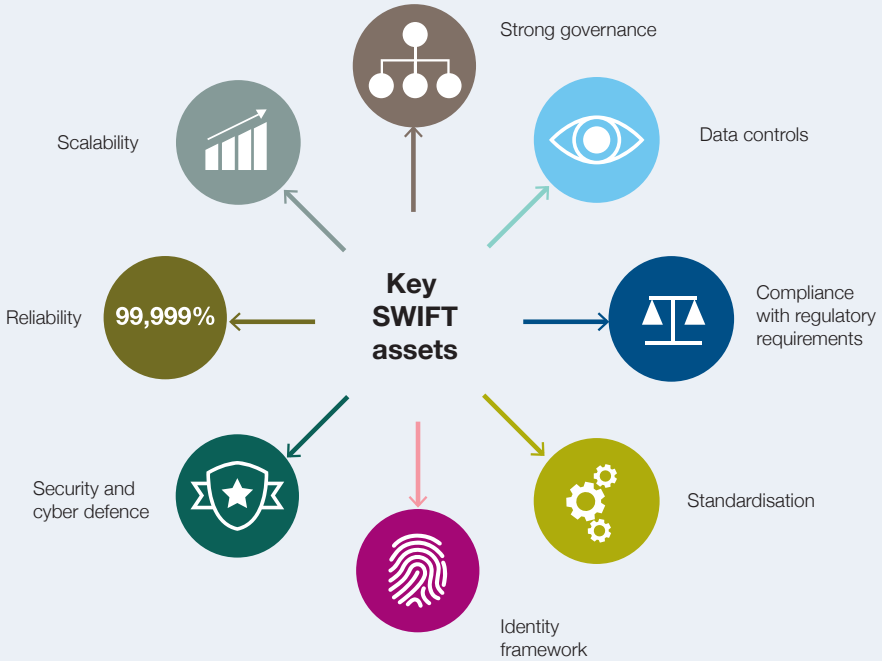


- Research at very early stage but to a large extent, not yet addressed
- Addressed very partially; no clear trend on best resolution strategy
- Promising development, but significant R&D work still required
- Solution emerging, but industry validation still required
- Meeting financial industry requirement

Leveraging SWIFT's capabilities to deliver industry-standard DLTs

As a financial industry cooperative, SWIFT's focus is on building technical, operational and business capabilities with a view to evolving our platform such that DLT-based services could be offered to our 11,000+ members, when the technology matures and firm business use cases emerge. Our work is focused at addressing the identified requirements to ensure that future distributed ledger based services delivered by SWIFT are in line with the needs and expectations of the financial industry, guaranteeing end-to-end automation and backward compatibility with legacy processes.

SWIFT has been delivering solutions for the financial industry for the past 40+ years, and, in this context, has addressed many of the challenges identified in its existing products and services. Thanks to this, SWIFT holds a unique set of assets and capabilities around strong governance, unrivalled standards expertise, operational efficiency, security, reliability, and reach, which we will leverage to develop DLT services that meet the needs of our community.



Leveraging SWIFT's capabilities to deliver industry-standard DLTs

Governance and access control

As an industry cooperative, SWIFT has a unique governance model driven by its community to solve industry-wide issues. As such, SWIFT's governance has been designed to ensure that we play a utility role, facilitating financial transaction exchanges within the industry, with the purpose of serving our community rather than maximising profit. SWIFT governance is supported by a very clear definition of roles and responsibilities and by a very comprehensive framework allowing service administrators to offer their services via SWIFT in order to control access, and define authorised participant interactions through the definition of closed user groups or RMA authorisations.

Data Controls

SWIFT systems and processes are designed, built, operated and maintained to guarantee the confidentiality of the data of our community. Data is being encrypted on multiple layers and very strict controls apply to restrict data access in line with a set of well-documented policies. Our compliance with these policies is audited externally on a yearly basis and details are made available to the SWIFT community as part of the ISAE3000 report.

Compliance with regulatory requirements

At the request of its community, SWIFT is heavily investing in building a complete compliance portfolio for its community. Compliance is a challenge shared by all financial institutions, and one that is best met together. Since investments in financial crime compliance do not yield competitive advantage, it makes sense to collaborate to mitigate costs and risks for all parties.

Standardisation

SWIFT Standards brings together a unique and proven combination of capabilities for defining business automation standards vital for any industry application of DLTs. SWIFT's work in ISO 20022 standards, its business knowledge, and know-how of the various financial markets – as well as its relationships with the financial industry and ability to convene and manage industry groups – have all greatly contributed to the high level of standardisation observed across today's financial industry.

Identity framework

SWIFT services use advanced cryptographic features to ensure identification, traceability and accountability of all actions performed. Financial institutions are identified through their BIC and transactions are digitally signed using PKI keys which are certified by SWIFT certification authority allowing participants to confidently trust that their counterparty is genuine. Key management operations are supported by very robust and secured processes, allowing services to be operated efficiently and situations in which keys are either lost or compromised to be resolved via certificate recovery and revocation facilities.

Security and cyber defence

Security has been part of the SWIFT DNA from its inception; all the cyber defence mechanisms protecting SWIFT's secure IP network are equally relevant in a DLT context, and can be leveraged to allow participants to safely conduct their business on a protected peer-to-peer private secured network.

Reliability

SWIFT is well known for its record high availability[1], its extensive business continuity plans, and for its ability to deliver mission critical software for the financial industry. It manages industry-wide migration smoothly, with interoperability and backward compatibility between versions guaranteed. This know-how and expertise can be leveraged in the DLT context, and is undoubtedly an important quality required of any credible solution provider.

Scalability

Today SWIFT supports very high volumes of traffic on its various messaging services[2]; volume generated from a wide variety of financial institutions located all around the world, delivering services supporting payments, securities, FX, and trade finance business. SWIFT has scaled its systems in line with its community requirement, while keeping availability at the highest level.

Reach and integration with legacy systems

SWIFT's secure IP network has a very well established presence within the financial industry with more than 11,000 financial institutions connected to date – making it the natural choice for the provision of a secure DLT-based service. Our messaging and integration portfolio offers a wide range of solutions designed to facilitate the connection with customers' existing back-office systems, and can be reused to bridge the new DLT-based services with legacy systems inside a financial institution.

Supporting industry transformation

The adoption of distributed ledger technology is unlikely to happen through a big bang migration. With the extensive set of legacy systems in place today, adoption of distributed ledger technology will not just require a technology shift but would also imply a degree of business transformation. Such processes take time, and not all businesses and parties progress at the same speed. Therefore, it will be necessary to ensure that adoption takes place at a steady pace to avoid the costs of running parallel systems for an extensive period of time.

In this context, our experience in managing community-wide transformation is valuable. SWIFT has migrated its community successfully on a number of occasions and across multiple technology revolutions in a smooth and timely fashion. This was achieved through a combination of communication, planning and execution skills; all leveraging SWIFT's governance structures, and the relationships developed over a considerable period with our customer and vendor community. The very same principles could also be applied in a DLT context.

1. 99,999% availability for SWIFTNet and FIN messaging services in 2015
2. 6.1+ billion FIN messages in 2015

SWIFT's R&D on DLTs

As part of its R&D activities, SWIFT is actively experimenting with DLTs and is working on a number of initiatives, including:

Community engagement

SWIFT has dedicated significant resources to engage with its community, exploring business use cases in the securities, payments, trade finance and reference data areas, where DLTs could bring real business benefits over existing solutions. Principally, this has been done through bilateral discussions with dozens of financial institutions.

Linux Foundation's Hyperledger Project

SWIFT is both a Founding Member & Board Member of this open source project aimed at advancing DLTs. SWIFT is working in collaboration with this community to build the foundation of a production grade distributed ledger implementation which can address the known issues and limitations of current implementations. SWIFT is also actively experimenting with technologies in the Ethereum ecosystem of products.

Proofs of Concept

A number of DLT-related Proofs of Concept (PoC) are ongoing in SWIFT Innovation Labs to further increase our knowledge and expertise, and validate the SWIFT approach to building a platform which is agnostic of business use cases. The following PoCs are currently being worked on:

- **Identity and Access Management** – This PoC integrates a DLT solution with a SWIFTNet PKI solution and access control mechanism (such as a closed user group and RMA) to demonstrate how SWIFT can leverage its existing platform and assets to solve the identity and access management issues highlighted as part of our technology assessment.
- **Standing Settlement Instructions (SSIs)** – This aims at demonstrating the benefits of DLTs by building an SSI database for OTC markets in a reference data context in which there are no data confidentiality concerns. The PoC also explores interoperability and backward compatibility with existing SSI solutions such as the MT670/671.
- **ISO 20022** – This PoC aims at applying SWIFT standards expertise and the ISO 20022 methodology to the DLT context. It is assessing how interoperability with legacy systems can be achieved when not all stakeholders are on the distributed ledger. The bond lifecycle from issuance to asset service has been taken as an illustrative example, as a bond is a simple but relevant securities asset class to demonstrate SWIFT's capabilities.

More PoCs have been, or will be, launched in order to further develop SWIFT's capabilities to support DLT-based solutions on its platform. The areas covered in the PoCs should be considered as illustrative to prove the capabilities of the technology and support SWIFT's work to build a DLT platform which is standardised and use case agnostic.

SWIFT's R&D on DLTs

Standards

The SWIFT Standards team is investigating DLTs to understand how existing messaging and reference data standards can be re-used in a DLT context. Re-use of existing standards is important for two reasons:

- First, to avoid 're-inventing the wheel': existing standards such as ISO 20022 contain precise, industry-ratified definitions of business concepts that can be transposed to DLTs and accelerate solution implementation.
- Second, to facilitate end-to-end business processes: it is unlikely that a complex business process will be scoped to a single DLT environment. Rather, DLTs will interact with existing automation mechanisms, including messaging and APIs, and with other distributed ledgers. For this to occur safely and seamlessly, consistent, cross-referenced definitions will be required between DLTs and existing platforms where business standards are already widely deployed.

The SWIFT Standards team is also considering what a business standard dedicated to DLTs would look like. DLTs are different from messaging, and, although there is much in existing standards that can be re-used – from business content to governance processes – DLTs bring a number of new challenges for formalising and standardising business automation.

SWIFT Innotribe

Our Innotribe programme has launched the 'Innotribe Industry Challenge', which brings together SWIFT Member Institutions, FinTech companies and SWIFT internal teams to address obstacles and opportunities facing the industry. The output of these Innotribe Industry Challenges will be a number of Proofs of Concept, which will enable us to collaboratively explore, and design utility solutions; the first Innotribe Industry Challenge will investigate securities issuance and asset servicing on DLTs.

The SWIFT Institute

The SWIFT Institute, which funds independent financial industry research, is to publish two academic research papers on DLTs in 2016; the first will focus on: "The Impact and Potential of Blockchain on the Securities Transaction Lifecycle".

The global payments innovation initiative (gpii)

As part of the gpii, SWIFT is working collaboratively with more than 50 of the world's largest transaction banks to drive the long-term vision for correspondent banking and investigate their potential joint role in deploying new technologies such as DLTs. Throughout Q2/Q3 2016, 'Vision Workshops' will be held with gpii initiative banks, as well as SWIFT's banking and payments board committee. The outcome will be a draft 'vision' and roadmap for the future of correspondent banking to be presented at Sibos in September 2016 for wider debate in the industry.

About SWIFT

SWIFT is a cooperative of and for the financial community – a trusted provider with our sights on serving the industry in new and ground-breaking ways.

To find out more about SWIFT's work on distributed ledger technologies, please contact DLT@swift.com

For more information about SWIFT, visit www.swift.com


swiftcommunity


company/SWIFT

Disclaimer

SWIFT supplies this publication for information purposes only. The information in this publication may change from time to time. You must always refer to the latest available version.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders.

For more information about Accenture, visit www.accenture.com


@Accenture


Accenture

Frédéric Le Borne
Managing Director
SWIFT Global Relationship Lead
frederic.le.borne@accenture.com

David Treat
Managing Director
Capital Markets Blockchain Global Practice Lead
david.b.treat@accenture.com

Fernand Dimidschstein
Managing Director
FinTech Innovation Lead
f.dimidschstein@accenture.com

Chris Brodersen
Accenture Research Principal
Capital Markets Blockchain Lead
c.brodersen@accenture.com

Disclaimer

Accenture's role in the paper has been limited to the provision of insights and expertise with regards to the current level of maturity of distributed ledger technology and its key functionality and strengths. While we take precautions to check that the source and the information we base our judgments on is reliable, we do not guarantee that this source and this information are accurate and/or complete and it should not be relied upon as such. The conclusions and recommendations provided in the paper represent the views of SWIFT and cannot be attributable to Accenture.

57189 - April 2016