The Advent of "The Internet of Value"

The potential of Blockchain and Distributed Ledger Technologies to reshape the financial industry

May 2018 / Version 5.0

Jorge Lesmes - jorge.lesmes@everis.com
Pilar Ejarque - pilar.ejarque@everis.com

Abstract: The economic landscape is undertaking a fundamental transformation. Financial services are facing unprecedented challenges; augmenting demands from customers and shareholders, heightening pressures to drive continued cost efficiencies and ever intensified regulatory requirements to encourage fair competition and transparency. The traditional "winner takes all" concept leaves place for a new reality; a "co-opetitive" environment where companies must compete and collaborate to remain relevant in this networked economy.

As a result, the industry calls for agile and scalable methodologies. The disruptive concept of Blockchain & Distributed Ledger Technologies (DLTs) presents unrivalled opportunities to deliver these imperatives. These technologies (extensively described in this whitepaper) have the potential to disrupt the industry's *status quo* in the same way that the Internet did in the 90s, introducing the revolutionary "The Internet of Value" concept and transforming the competitive dynamics of the banking industry by offering new ways to connect customers.

Nevertheless, a multitude of competing platforms co-exist with no clear winner, highlighting the need for a de-facto interoperability standard that enables creating a unified financial ecosystem. Moreover, the need for a secure and self-sovereign management (customer owned) of the Digital Identity of citizens and corporates is also becoming the single point of failure (e.g. cybersecurity, repetitive KYC & on-boarding) and friction (e.g. delays of on-boarding) of this whole technological transformation. Only when these concerns are resolved, "The Internet of Value" era can become a reality.

Table of Contents

1. Introduction

Technology is transforming the way customers access services. The internet is connecting supply and demand more effectively than ever before, and at a fraction of the cost. In particular, Blockchain and DLT platforms have grown in prominence and been recognised as a potential game-changer for many industries, including the financial services. These technologies are expected to greatly impact the way assets are exchanged and significantly reduce the operational costs for banks and other financial institutions by introducing "The Internet of Value".

"The Internet of Value" concept uses "The Internet of Information" analogy to explain how Blockchain and DLT have the potential to disrupt our lives in the same way that the interconnection of networks of information did in the 90s [1]. Similar to how the Internet of Information, created over open standards, fostered the creation of new business models like Facebook and Uber for consumers, "The Internet of Value" uses open standards to bring a new tool to share and manage the value of assets (of any type) without the need of trusting a governing central entity. With "The Internet of Value", a value transaction such as a foreign currency payment, can happen instantly, just like people have been sharing texts, images and videos online for decades. And not only money, "The Internet of Value" will enable the exchange of any asset that has value (financial assets), including stocks, titles of ownership, votes and intellectual property, among others.

In order to understand the potential for Blockchain/DLT to transform the financial industry standards and introduce the "Internet of Value", it is important to analyse the concept. Blockchain technology refers to a set of technologies and different fields of science that grouped together enable the storage & exchange of data in a decentralised and secure manner where no central regulator is required. The terms Blockchain and DLT are commonly used interchangeably. Nevertheless, a fundamental distinction between them exists. A Blockchain platform, such as Ethereum or Bitcoin, refers to the traditional chain of transactional data blocks interlinked where one global distributed ledger exists. As a result, every participant of the network accesses the same source of truth irrespectively of their geographical location. The traditional Blockchain infrastructure (which replicates all encrypted transactions in the network nodes with fully open access) is however imposing architectural limitations to meet the restricted and carefully specified data sharing

requirements of the financial industry. The need for an infrastructure capable of exchanging information only among relevant parties (safeguarding privacy and scalability) becomes apparent. DLT platforms, such as Corda or Hyperledger Fabric, are designed to fulfil these standards in order to facilitate technology's widespread adoption [2].

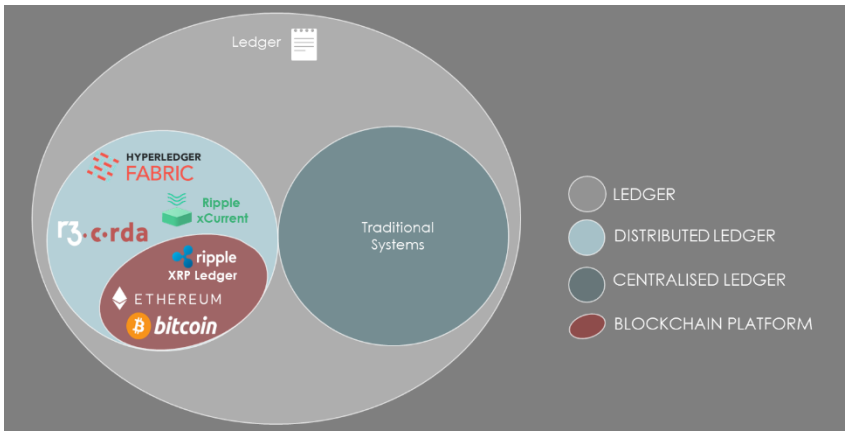


Figure 1. Overview of the Blockchain & DLT concept

The financial industry is undertaking a structural change towards more strategically focused, technologically adaptable, and operationally agile institutions that are able to remain dominant in a continuously evolving ecosystem. This evolution is far from easy as most organisations confront numerous challenges; complex and diverging regulations, legacy systems, disruptive models and technologies and, last but not least, a customer base with ever higher expectations [3].

New regulations are fundamentally changing the payments value chain, in an attempt to stimulate competition, increase transparency and reinforce customer protection. For instance, the Second Payment Services Directive (PSD2) requires banks to open their payments infrastructure and customer data assets to third parties that can develop payments and information services to customers. Importantly, regulatory directives should not be considered as a sole compliance concern, but a reason to improve current business prepositions [4]. Blockchain technologies can play a pivotal role in the implementation of these regulations by reducing the implementation efforts and friction points.

Moreover, these industry changes are enabling new players with transformative business models to access the market and capture significant revenues. Without the

legacy infrastructure restraints and associated costs, these entrants are able to provide alternative mechanisms, which are faster than traditional banks. For instance, neo-banks such as Monzo or Starling are rapidly penetrating the market thanks to their accessibility and customer focus. As a result, incumbents need to address the challenges of complying with these regulations, meeting changing consumer demands and implementing disruptive technologies, while improving service resilience and security for an increasingly global payments network. More importantly, these changing business dynamics make the collaborative value inherent in "co-opetition" more necessary than ever. Companies need to establish market strategies that capitalise on relationships in order to create maximum value in the marketplace [5].

Nevertheless, despite the numerous challenges that the financial industry is facing, our experience in the implementation of Blockchain and DLT solutions in the banking industry has enabled identifying two main conundrums that financial institutions are facing that are however commonly underestimated by the market, both from the theoretical and practical point of view. These referring to the need for a Self-Sovereign Digital Identity Management system that transforms the current on-boarding process and the lack of interoperability among competing platforms & systems.

The purpose of this document is hence to outline the current scope of Blockchain and DLT by analysing the revolutionary "Internet of Value" concept and its potential in disrupting distributed environments with multiple market participants. The report will underline two commonly overlooked challenges in the financial industry; ***Identity Management*** *(section 2) &* ***Interoperability*** (section *3)* and provide a comparative analysis of how traditional and innovative technology–such as Blockchain/DLT platforms- aim to resolve this market friction.

2. Self-sovereign Digital Identity Management for Corporate On-boarding

2.1. Context and Motivation

Corporate on-boarding, along the subsequent KYC and AML compliance, represents one of the most critical areas for financial organisations, given its direct impact on

client experience. On-boarding represents the first interaction a customer has with a financial institution, hence, the starting point to create long-term loyalty. Nevertheless, over 64% of banks report lost deals and revenue due to problems in the current corporate on-boarding process [6]. This may not be a surprise if we consider the current compliance costs. The average cost figure for financial organisations to meet their obligations is $60 million (with some banks spending up to $500 million) on compliance with Know Your Customer (KYC) and Customer Due Diligence (CDD) [7] and the global spending on Anti Money Laundering (AML) compliance is estimated to amount $10 billion [8].

As the aforementioned figures suggest, compliance with current KYC regulations proves expensive, inefficient, and more importantly, poorly customer oriented. It can take up 30 to 50 days (+60 in case of large corporations) to complete all the necessary checks, including the numerous pieces of documentation that need to be produced and verified [9]. As a result, it is estimated that more than 80% of the effort associated with KYC is dedicated to information gathering and processing, with only 20% focused on information assessment and monitoring [10]. The reason for the length of this process relies on the necessity to satisfy the latest customer due diligence regulations and compile extensive manual documentation. Moreover, the traditional process is highly repetitive, obligating customers to undertake the same screening analysis and KYC checks by answering the same questions every time they wish to enrol in a different financial entity.

Hence, the process does not only represents an arduous process for corporate clients, but a huge burden for banks; who face astronomical fines for incorrectly discharging KYC responsibilities. In the last 5 years, more than a dozen of global banks have paid excess of $15 billion for AML and KYC violation laws. Consequently, banks are coming under pressure to reduce costs and improve customer experience. Nevertheless, compliance budgets are expected to increase in the following years rather than to decrease, as firms overhaul systems and digital solutions' expenditure rises [11].

Considering these numbers, it is clear that the financial industry necessitates a profound re-evaluation of the traditional corporate on-boarding process and the subsequent KYC & AML check procedures. A comprehensive corporate on-boarding tool that complies with the current KYC, AML processes and the Regulatory

Directives such as FATCA, MiFID II, GDPR and ACAMS is required. A move from a lengthy, paper-based and inconvenient process to a smooth and genuinely omni-channel client experience is clearly a true game changer for the industry.

2.2. Market Solutions for the Onboarding Conundrum

2.2.1. Traditional Technologies

The traditional response for the financial sector to this concern has been to build ever higher walls around the organisations' and clients' assets, centralising information into legacy silos, with a single entity controlling the system. Every bank and financial institution requires performing the KYC process individually, and upload the validated documentation into the central registry that stores digitised data tagged to a unique identification number for each corporate customer. By using this reference number, banks access the stored data to perform due diligence whenever customers request for a new service within the same banking relationship, or from another bank. This however creates a single point of failure, as instead of securing the data into distributed environments where risk is minimised, centralised identity management models (IdM) face strict challenges due to the increasing regularity of data breaches that lead to reputation damage, identity fraud, and more importantly, significant loss of privacy. Moreover, these events highlight a lack of control and ownership that end-users experience with their digital identities, and hence, a need for a self-governing identity form.

The concept of self-governing identity represents an evolution of the concept of identity where the user is central to the administration of identity [12]. That is, rather than simply encouraging users to be at the centre of the identity process, self-sovereign identity requires the users to govern their own identity; advocating user autonomy.

Figure 3. The evolution of online identity

The move to self-sovereign identity is a move from a silo mentality to a layer mentality, as *Figure 4* illustrates. Conventional approaches to identity have always struggled with portability, precisely because data is held in multiple closed silos repositories. Complex mechanisms and competing standards have emerged to move

data from one silo to another, but without obtaining significant market traction. While silos persist, customers will remain dependent to the organisation that owns and manages their data for them.

Nevertheless, as result of the flourishment of self-sovereign identity, the new post-silo world can become a reality. This will transform how rather than every organisation maintaining their own siloed store of user data and possibly a suite of APIs to connect to other such silos, each organisation can have one single connection to the Identity Data layer, and immediately benefit from all the organisations that are already present [13].

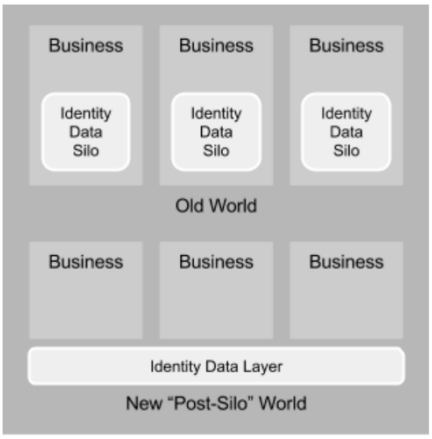


Figure 4. The New "Post-silo" World

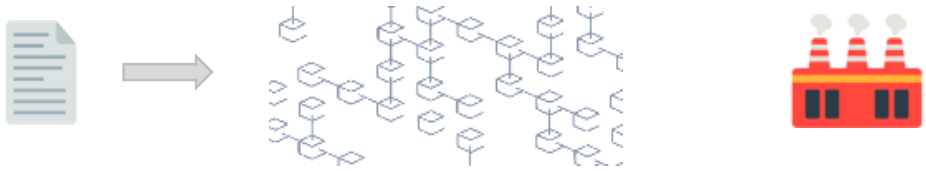
As a result, although traditional technologies may had been the answer in the past, they are starting to face challenges in this interconnected digital world. These approaches are proving inadequate for modern financial services operations. This is because although they are trying to mitigate the inefficiencies of system, they are not targeting the fundamental problem; *digital identity portability across organisations to facilitate corporate KYC and AML verification*. In other words, traditional technology does not offer users the opportunity to manage their identity in a decentralised and distributed manner.

2.2.2. Innovative Technologies

The adoption of Blockchain/DLT technology could lead to a significant reduction of AML and KYC costs thanks to its cross-institution client verification capability and

its effectiveness in monitoring and analysing data required for AML and KYC checks. Blockchain technology proposes to enhance decentralisation, transparency and user control in transactions that involve identity information, resolving frequent KYC, risk profiling and AML issues through a shared distributed infrastructure [14]. With a blockchain-based registry, a distributed database of verified customer data, client and transaction legality only need to be performed and validated once, with the final result being cryptographically stored in the platform. That is, once the information is verified, it is published across all participant nodes that have been given permission to access data by the customer. Hence, when a corporate approaches a new bank to open an account the bank will be able to access their pre-verified information from their node on the blockchain. This is not too dissimilar from the model today but assumes that all banks would use one blockchain network (as opposed to multiple KYC utilities), and would enable near real-time dissemination of updated, verified customer data to all banks, as well as benefitting from the inherent increased security that blockchain delivers through cryptographic hashing [15].

As *Figure 5* illustrates, the key point is to enable creating a company Blockchain network of identities where authorised organisations can query information to facilitate corporate on-boarding, reducing time and increasing client retention. As a result, different financial institutions can access user information, assuming user provided consent to data, and facilitate the portability of users' identity across organisations. This will allow for the empowerment of people with personal data storage and management as well as the creation of permissioned frameworks for relevant third parties to access information; radically transforming the corporate on-boarding experience.



We use digital on-boarding to capture all personal details from the individual and create a digital token of their information which gets stored in the Blockchain network.

The digital token is exchanged through the Blockchain network, which supports different levels of information interchange:

- Aggregate information of several users (creating segments)
- Anonymized information for a specific user: only the gender, age, economic level, financial scoring…
- Full ID: detail personal data (having the user consent)

Companies which are part of the network can interact with the digital token of the user in a digital way, substantially reducing the amount of required paperwork that customer on-boarding usually requires.

Figure 5. On-boarding Use Case

As a result, a blockchain-based registry is able to remove the duplication of effort created by the multistep AML & KYC processes, providing final and immutable results recorded in a decentralised ledger. Moreover, the ledger enables encrypted updates to client details to be distributed to all banks in near real-time and provides a historical record of all shared documents and compliance activities undertaken for each client. Hence, since all of the information related to a client becomes available to those organisations that hold appropriate permissions, a single source of "truth" is created, resulting in a much simpler, less time-consuming and cost-effective manner to process corporate compliance verification [16].

Moreover, the real selling point of using blockchain is the ability to create, and subsequently use, a self-sovereign digital identity. By creating an identity on the blockchain, the user becomes the governing authority, obtaining greater control over who has their personal information and how corporates, and especially banks, access it [17]. Hence, once a corporate´s KYC and AML documentation has been verified, a digital identity can be created for that customer –attached to every transaction they undertake, as a way of signing transactional data-. This digital identity will store all relevant customer information (addresses, account details, director's details, PEPs, etc) that can be used during AML/transaction monitoring, hence, increasing monitoring accuracy and reducing the likelihood of false validations. In addition, those financial institutions that identify a fraudulent transaction can distribute the details of that transaction globally to all connected banks; minimising the risk for further fraud.

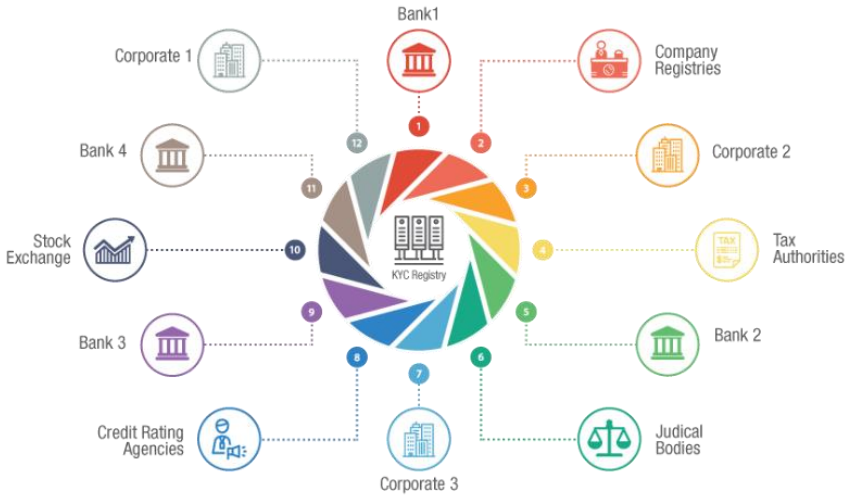


Figure 6. Corporate KYC Registry participants

Some interesting examples that take into consideration the need for a Self-Sovereign Digital Identity include Estonia e-Residency ID; which enables citizens to access services including health and pension records, medical prescriptions, and voting information using their digital ID record [18], and Alastria, the Spanish multi-sectoral Blockchain Consortium, that utilises a digital identity model to enable an adequate mechanism of knowledge of the people, organisations and users of the network and their services, facilitating the establishment of relationships with full legal effectiveness across the consortium participants [19].

2.3. Applicability to UBS Athena

Considering UBS Athena distributed corporate environment where multiple financial entities take part, an effective and straightforward Identity Management solution that enables verifying corporate KYC and AML is required.

UBS Athena can take the opportunity to break barriers for traditional data exchange, by implementing an advanced blockchain-based solution that manages the portability of client identities in a distributed environment. That way, banks joining Athena do not longer need to perform their own KYC/client on-boarding but can make use of their self-sovereign digital identity to verify compliance requirements. This will enable reducing the likelihood of errors while creating an "auditable" trail to satisfy regulators by providing data clarity and context.

everisID directly targets this matter by creating a Self-Sovereign Digital Identity system that facilitates the on-boarding process in a multi-player environment. Please refer to the section 5.1. in the Appendix for further detail.

3. Interoperability among Blockchain platforms and traditional ledgers

3.1. Context

At everis and NTT DATA, we believe that Blockchain and DLT platforms have an inexhaustible potential. We envision a future where value is recorded and automatically managed and exchanged without error, creating a seamlessly experience where no friction exists. The need for expensive reconciliation, duplication, inaccurate matches and breaches will become a matter of the past. Markets will move towards models where financial agreements, represented by smart contracts[i], are only recorded once (though distributed and decentralised), encouraging a collaborative effort between participants in order to maintain accurate and shared records of these agreements. For instance, *Figure 7* illustrates a real case scenario where market rivals collaborate with each other to create an

asset servicing and communications marketplace for syndicated loans where every agreement is mapped and stored in a smart contract.

We believe there will not be a single platform or vendor that governs them all, but different platform winners depending on the specific business case. A wide variety of Blockchain and DLT platforms exist at the moment. Platforms vary depending on codebase (open-source or proprietary), network (permissioned or permission-less), the technology stack implemented and the consensus method (e.g. Proof of

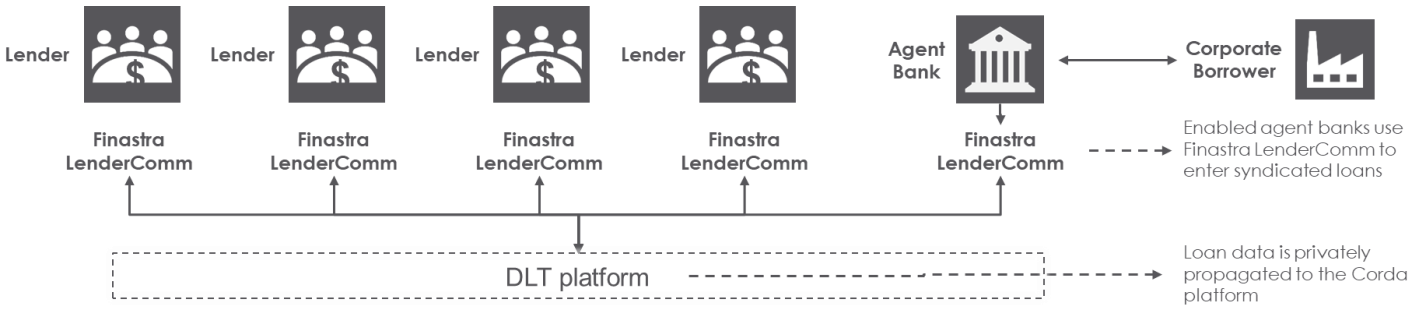


Figure 7. Example of a Syndicated Loans Settlement online marketplace

Work, Proof of Stake). Hence, a platform may be more suitable to a particular market than others. As a result, Blockchain and DLT platforms have acquired a specific focus in their approach, aiming to achieve a specific target rather than attempting to become the solution for every business problem. For instance, Ripple aims to evolve into the leading cross-border payments DLT solution, and Chain, Hyperledger Fabric and R3 Corda have built precise systems that target the strong privacy and scalability concerns of the financial industry. Nevertheless, the existence of a multitude of competing Blockchains which do not necessarily connect with one another, makes it impossible to connect assets like information –for now-, and hence, prevents "The Internet of Value" becoming a reality.

3.2. Solutions

For this to occur, industry standards must be adopted in order to homogenise the world's different financial systems.

Ledger systems today are siloed and disconnected. Transfers of value are relatively easy within one country, or if the sender and recipient have accounts on the same network or ledger. But sending value to someone on a different network or ledger is

complex and often impractical. Where connections between ledgers do exist, they are manual, slow or expensive [20].

As a result, we envision a future where a de-facto interoperability standard sets the rules of the game, facilitating the interaction across multiple completing platforms and devices.

3.3. Applicability to UBS Athena

Considering how UBS Athena aims to address the necessities of a discrete set of audiences, functions and asset classes through a client interface that offers a wide array of technology platforms, a de-facto interoperability standard that connects the multiple competing systems would be extremely useful. UBS Athena nature as a system aggregator for multiple back-end processes will necessitate an API gateway that is able of interconnecting multi-diverse applications and technologies, especially as many of these services may be based on Blockchain and DLT technology.

everis is co-leading the development of *Interledger (Hyperledger QuILt* when incorporated to the Hyperledger Consortium*),* that can target UBS Athena's interoperability conundrum by offering a gateway between existing payment systems and innovative Blockchain, DLT platforms. Similar to how Athena generates a layer of abstraction across a wide set of different platform features and services, Interledger offers a layer of abstraction across competing Blockchain/DLT and traditional ledgers. Please refer to the section 5.2. in the Appendix for further detail.

4. Conclusion

The future is uncertain, but promising. "The Internet of Value" revolution will not happen overnight, but action needs to be taken now. For this technology to have a long haul in the financial industry, cooperation between market participants, regulators and technology experts is a must. Only then it will be fruitful.

It is important to understand the how the financial industry is evolving and analyse the best courses of action for the ongoing challenges; customers´ augmenting

demand, intensified regulatory requirements and technological disruption that calls for "co-opetition" across market participants. This paper acknowledges the radical transformation the financial industry is undertaking and focuses on two of the main conundrums of the industry, the need for a Self-Sovereign Digital Identity Management system that transforms the current on-boarding process and the lack of interoperability among competing platforms & systems.

As this paper mentioned, there will not be a Blockchain or DLT platform that governs all others, but different winners depending on the specific use cases. That is, while some platforms are better adapted to the needs of financial markets, others will offer a greater benefit in terms of digital identity (typical public-sector organisations) or international payments. The user will make their choice depending on the use case they intends to solve. As a result, a multitude of competing platforms will co-exist, and the need for an interoperability standard will become apparent. The future calls for interconnectivity and global collaboration.

The scope of "The Internet of Value" is yet to be defined but promises to be extraordinary. As a result, there is no better time to start "The Internet of Value" revolution than now.

5. *Appendix*: everis and NTT Data approach to Identity Management and Interoperability

everis and NTT DATA are co-developing solutions for tackling these fundamental challenges: *Hyperledger QuILt*, a suite of protocols that offer an interoperability gateway between competing Blockchain, DLT platforms and traditional ledgers; and *everisID*, a solution for self-sovereign Digital Identity Management.

5.1. everisID: A solution for Self-Sovereign Digital Identity Management

5.1.1. Our Vision

Our solution *everisID* acknowledges the potential for disruption in this sphere and offers a self-Sovereign Digital Customer Identity and Authentication Management capable of transforming the highly inefficient on-boarding process of financial institutions. *everisID* offers a solution to manage users' identification in a

multiplayer environment that improves and simplifies the interchange between different organisations of users' identification in digital ecosystems by using a Blockchain network. The current version has been developed in Ethereum and it is designed for B2C (Retail) and a B2B version (SME and Corporates). Nevertheless, in order to facilitate widespread adoption, migration to Hyperledger Fabric and R3 Corda are in progress.

By combining the decentralised Blockchain principle with identity verification, this solution aims to facilitate the on-boarding journey by improving customer experience, increasing security and enhancing bank's efficiency. Thanks to this Blockchain infrastructure, ID interchange between multiple organisations is simplified; customers simply rely on user-friendly applications for authentication and can access personal information anytime they want. *everisID* stores their encrypted identity, allowing users to share and manage their data on their own terms. Hence, letting the user become the sovereign owner of this information.

As a result, *everisID* enables the creation of an ecosystem suitable for new business models where the bank becomes the provider of trust to its customers. It offers an innovative client experience where the customer is put at the centre of the banking activity.

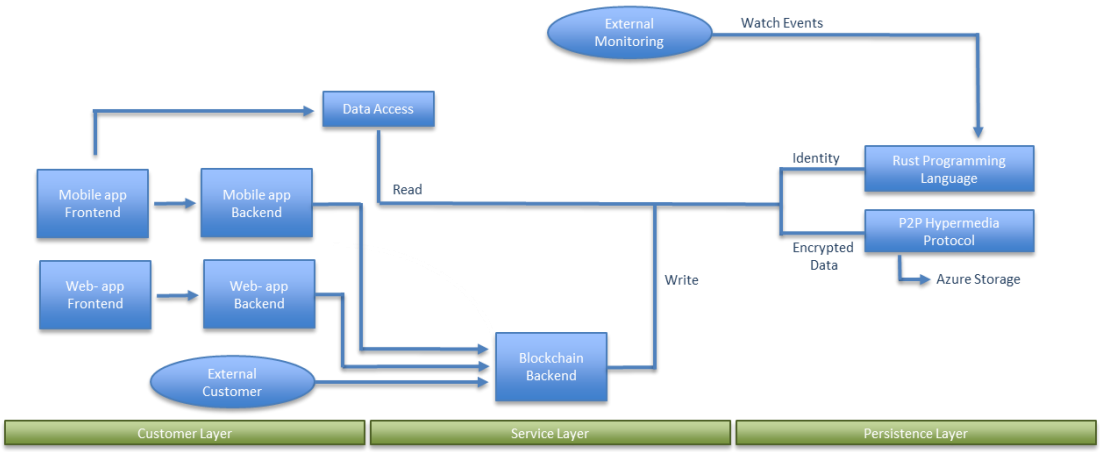


Figure 8. Architecture Design for everisID

5.1.2. Business Use Case: Client on-boarding based on a DLT platform

everisID aims to improve and simplify the customer experience by offering a full online boarding experience where customers are guided through the process on a simple and clear interface. This process starts with the user fulfilling key personal details and validating their digital identity by online channels.

To create an identity in the *everisID* application it is necessary to establish an authentication channel with the Authoriser sending the user information. The Authoriser using a *JSON Web Token* (JWT) to secure the communication, will return a positive or negative status of the user. If the user status is confirmed, *everisID* will create the account into the Blockchain Network by encrypting the profile. The network will return a *Multi Network Identifier* (MNID), which enables safe-guarding Blockchain information in a multi-channel environment by encoding client addresses. To verify the profile has not been compromised within the communication channel, *everisID* will forward the MNID and JWT tokens to an *attester*, in charge of validating the profile. The attester will check the JWT and verify it is valid. Once the ID is verified, it can be used for other members of the network.

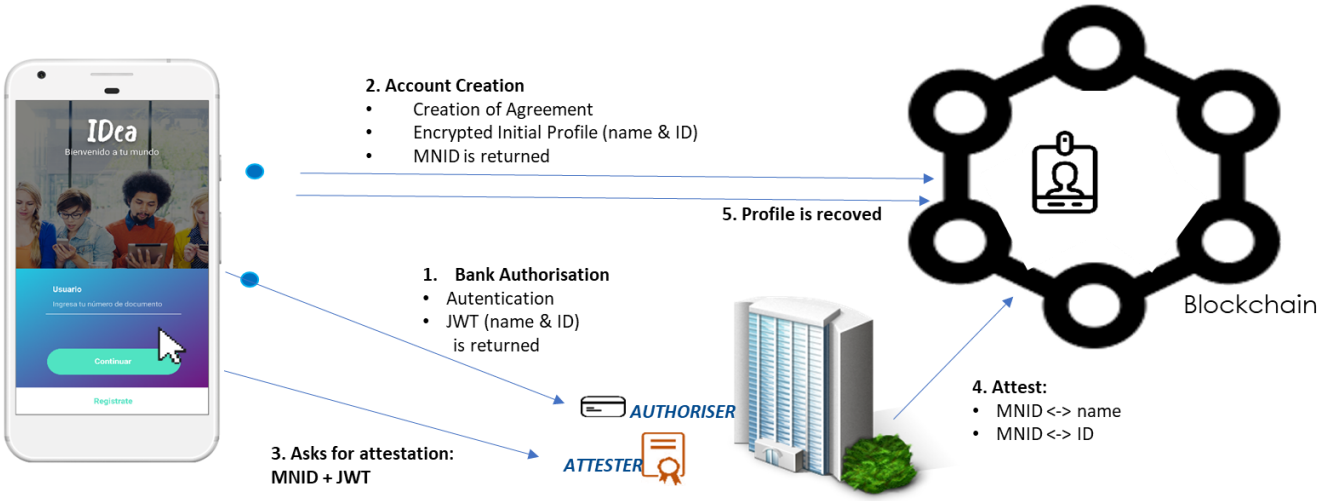


Figure 9. On-boarding Workflow Use Case

The purpose of this platform is that the core where all information persists in a blockchain that offers scalability, maximum security, efficiency and transparency that supports:

- Customers (of any service contracted by any company)

- Subscribers (of any company interested in consuming *everisID*)
- Collaborators (of any company interested in collaborating and contributing to the platform)

5.1.3. Product Roadmap

As a result, *everisID* provides a seamless and faster customer on-boarding process leveraging all the Blockchain advantages and connecting with the growing Fintech ecosystem. The solution stores the customer information in a digital token and opens the possibility to create new business models over Blockchain that are fully compliant with the new GDPR, Open Banking and PSD2 regulations.

5.2. HyperLedger QuILt

5.2.1. Context and Motivation

everis and NTT DATA are co-leading the development of the InterLedger Protocol [21], also known as ILP. InterLedger represents an innovative interoperability gateway which standardises how to instantly settle transactions across different ledgers and networks. In other words, it is a protocol for making transactions across ledgers, initially focused on packets of money across different payment networks or ledgers. ILP standards and specifications are being defined by the open source community under the World Wide Web Consortium umbrella [22].

ILP was initially designed in 2015 and has been incorporated to the Hyperledger Consortium [23] in October 2017, being reframed to *Hyperledger QuILt*. Hyperledger Consortium is a ”co-opetitive” initiative for launching Blockchain and DLT solutions across different sectors. It is important not to confuse the Hyperledger Consortium, with Hyperledger Fabric, a DLT platform initially incubated by IBM.

Hyperledger QuILt [24] is the Java implementation of the *InterLedger Protocol* adopted by the Hyperledger Consortium. It represents a simplification of previous versions of the protocol that is optimised for routing large volumes of low-value packets, also known as "penny switching". *QuILt* can be integrated with any type of ledger, including those not built on Blockchain and DLT platforms, and it is designed

to be used with a variety of higher-level protocols that implement features ranging from quoting to sending larger amounts of value with chunked payments. *QuILt* will act as a gateway between existing Blockchain, DLT and payments platforms providing a layer of abstraction [25].

ILP (and hence its java implementation; *Hyperledger QuILt*) is based on concepts dating back to the 1970s and 1980s, but it took the advent of Bitcoin and the global Blockchain movement to make the world realise that money and value transfers could be reinvented with Internet based technologies.

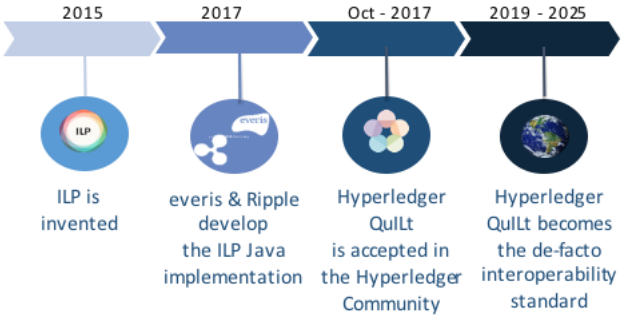


Figure 10. InterLedger Protocol / Hyperledger QuILt evolution

Hyperledger QuILt, aims to provide:

- A set of rules for enabling ledger interoperability with basic two-phase commit semantics for distributed transactions across multiple ledgers
- A standard for a ledger-independent address format and data packet format that will enable connectors to route transaction requests
- A framework for designing higher level use-case-specific protocols

5.2.2. Business Use Case: Interoperability of Blockchain, DLT platforms and traditional ledgers

Hyperledger QuILt aims to become the de-facto standard for interoperability. Just like the protocol HTTP evolved into the global standard for online information exchange, *Hyperledger QuILt* aims to become the standard for value exchange. The mission is clear; allow the user to transmit the value of any type of assets (and not just financial assets) with the same speed, ease and efficiency as a text is transmitted today. Internet protocols enable information to be packetized, routed and delivered over communication networks. With *Quilt*, money and other forms of value can be packetized, routed and delivered over payment networks and ledgers. *ILP,* and hence *HyperLedger QuILt,* is designed to be used in a layered protocol architecture, similar to how the Internet protocol stack was created [26].

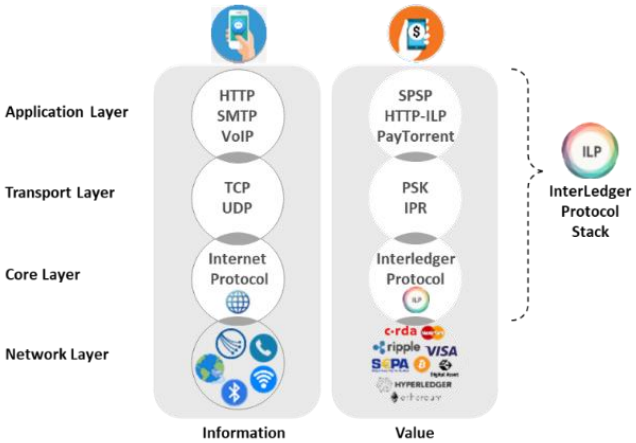


Figure 11. ILP's Analogy to TCP/IP

QuILt is highly suitable for a multiplayer environment by permitting members' DLTs, financial institutions private ledgers, IoT companies' wallets and supply chain solutions to interoperate with one another.

Using a Blockchain solution with distributed messaging protocol, it will be possible to create a shared ledger between trading counterparties to validate transactions in real-time moving money with the same speed, ease and efficiency as information moves today. That could be especially useful for complex financial assets with a no clear central authority to arbitrate or regulate them: Public & Private Stocks/Bonds,

Corporate Bonds, Derivatives, Syndicated loans, Factoring, and Derivatives Margin/Collaterals.

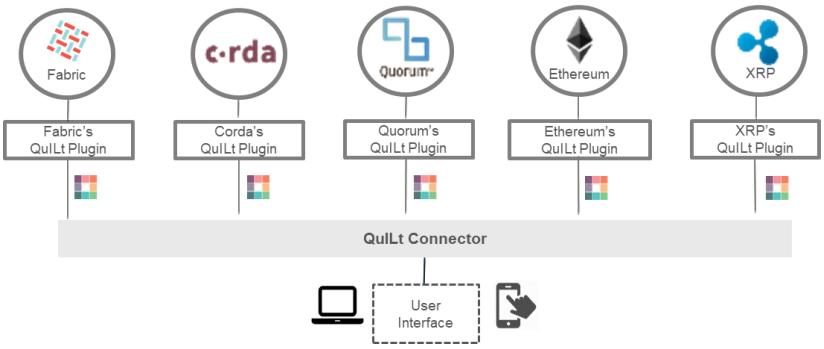


Figure 12. Hyperledger QuILt Connectors' Roadmap

5.2.3. Product Roadmap & Business Proposal

everis and NTT DATA have established a comprehensive business plan –*Figure 13*- in order to accelerate *HyperLedger QuILt*'s development. The objective is to build a rich ecosystem of ILP Java components and products that can be offered to financial institutions and technology companies.

Once the Standard Java Ledger Plugin & Connector Frameworks have been developed, they will set the foundation for the construction of interconnectivity components for DLT projects such as Hyperledger Fabric, R3 Corda, Digital Asset Platform, Ethereum, Quorum and other enterprise platforms: SAP, Salesforce, Bloomberg, Thompson Reuters, among others.

Figure 13. Business Model Offering Roadmap for Hyperledger QuILt

6. Bibliography

1. Leonard, S. (2017). *"The Internet of Value": What It Means and How It Benefits Everyone.* [online] Ripple. Available at: https://ripple.com/insights/the-internet-of-value-what-it-means-and-how-it-benefits-everyone/ [Accessed 9 Apr. 2018].
2. Brown, Richard Gendal, et al. (2016). *"Corda: An Introduction."* R3 CEV.
3. Deloitte (2018) *Banking Outlook: Accelerating the transformation*. [online] Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-dcfs-2018-banking-outlook.pdf.
4. European Commission. (2017). *Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments.* [online] Available at: http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm.
5. Bowser, J. (2018). *Strategic co-opetition: The value of relationships in the networked economy.* [online] Available at: http://www-07.ibm.com/services/pdf/the_value_of_relationships_in_the_networked_economy.pdf
6. Cognizant. (2013). Efficient Client Onboarding: The Key to Empowering Banks. [online] Available at: https://www.cognizant.com/InsightsWhitepapers/Efficient-Client-Onboarding-The-Key-to-Empowering-Banks.pdf.
7. Finextra Research. (2018). *How can Blockchain Help with AML KYC*. [online] Available at: https://www.finextra.com/blogposting/15https://www.finextra.com/blogposting/15022/how-can-blockchain-help-with-aml-kyc022/how-can-blockchain-help-with-aml-kyc
8. Yohannan, B. (2018). *Blockchain – A Blessing for KYC & AML?.* [online] Intellect: Design for Digital. Available at: https://www.intellectdesign.com/insight/blockchain-a-blessing-for-kyc-aml.html.
9. Finextra Research. (2017). *KYC and Blockchain*. [online] Available at: https://www.finextra.com/blogposting/13903/kyc-and-blockchain.
10. KPMG International. (2018). *Could blockchain be the foundation of a viable KYC utility?.* [online] Available at:

https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/03/kpmg-blockchain-kyc-utility.pdf.

11. Mac, D. (2017). *Corporate KYC pain: can the pain be eased? | Inside Financial & Risk.* [online] Thomson Reuters. Available at: https://blogs.thomsonreuters.com/financial-risk/risk-management-and-compliance/corporate-kyc-pain-how-can-financial-institutions-improve/
12. English, M. and Allen, C. (2018). *The Path to Self-Sovereign Identity.* [online] Available at: https://github.com/ChristopherA/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md.
13. Tobin, A. and Reed, D. (2017). *The Inevitable Rise of Self-Sovereign Identity*. Sovrin. [online] Available at: https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.
14. Jacobovitz, O. (2016). *Blockchain for Identity Management*. Available at: https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf
15. BCS Consulting. (2016). *Could blockchain solve the KYC/AML challenge?* [online] Available at: https://www.bcsconsulting.com/blog/new-technology-can-enable-human-bank/
16. Filippou, C. (2017). *Blockchain: A KYC-AML use case.* [online] www.blockchaintechnews.com. Available at: https://www.blockchaintechnews.com/articles/blockchain-a-kyc-aml-use-case-2/
17. Dunphy, P. and Petitcolas, F. (2018). *A First Look at Identity Management Schemes on the Blockchain.* [online] Arxiv.org. Available at: https://arxiv.org/ftp/arxiv/papers/1801/1801.03294.pdf
18. e-Residence. (2018). *Government of Estonia. [*online] Available at: https://e-resident.gov.ee/
19. Alastria. (2018). [online] Available at: https://alastria.io/#1 [Accessed 10 May 2018].
20. Dilley, Johnny, et al. (2016). "Strong Federations: An Interoperable Blockchain Solution to Centralized Third Party Risks." *arXiv preprint arXiv:1612.05491*.
21. Interledger.org. (2018). *Welcome | Interledger.* [online] Available at: https://interledger.org/ [Accessed 5 Apr. 2018].
22. W3.org. (2018). *Interledger Payments Community Group.* [online] Available at: https://www.w3.org/community/interledger/ [Accessed 5 Apr. 2018].

23. Hyperledger Consortium. (2018). *Hyperledger.* [online] Available at: https://www.hyperledger.org/ [Accessed 9 Apr. 2018].
24. Hyperledger. (2017). *Hyperledger QuILt.* [online] Available at: https://www.hyperledger.org/projects/QuILt [Accessed 9 Apr. 2018].
25. GitHub. (2018). *interledger/java-ilp-core.* [online] Available at: https://github.com/interledger/java-ilp-core [Accessed 5 Apr. 2018].
26. Hyperledger. (2017). *Hyperledger Gets Cozy With QuILt. [*online] Available at: https://www.hyperledger.org/blog/2017/10/16/hyperledger-gets-cozy-with-QuILt [Accessed 9 Apr. 2018].

[i] A **Smart Contract** is the digital representation of an **agreement** whose execution is both ***automatable*** by computer code working with human input and control, and whose rights and obligations, as expressed in legal prose, are legally ***enforceable***. (Clack, Bakshi and Braine, 2016).