Using blockchain as a digital identity

Daniel Maggs
Digital Currencies
Payments, Industry & Developement
Lloyds Bank

Cross-border payments are vital to the global economy and continue to rise in volume.

Due to recent improvements and support on industry commitment from initiatives such as the G20 and Swift GPI, cross-border payments have become faster and more transparent, with various friction points being reduced. Despite this, residual pain points remain.

Over the last decade, blockchain has been discussed at great lengths as a potential to revolutionise banking. Lloyds Bank has explored how exactly blockchain can be applied to the cross-border payments journey through the creation of a Digital Identity.

In this paper we explore how a digital identity could be created for corporate customers by banks and used to improve age old problems with KYC, Due Diligence and Sanctions screening. We then set out steps to taking this forward through the introduction of a framework for how this could work through a consortia-based model.

Globalisation has had many effects on the world economy, whether it be increased trade, the expansion of supply chains and entry into new markets for global corporates. All of this is facilitated through international payments, which are expected to grow from $150trn in 2017 to over $250trn by 2027 [1].

However, there remains persistent issues with international payments such as effective routing, transparency and high transaction fees that can culminate in delay and dissatisfaction to customers.

These issues have not gone unnoticed by the global industry, who together are aiming to solve these age-old issues. Indeed, we've seen commitment from G20 leaders, when in 2020, they endorsed a roadmap for cheaper, faster, more transparent, and accessible cross-border payments.

It's been noted that future work in this space will prioritise the following three, connected themes [2].

1. Payment system interoperability and extension
2. Legal, regulatory, and supervisory frameworks
3. Cross-border data exchange and message standards

The rollout and adoption of ISO20022 by the global banking community should enhance messaging consistency / standards as well as further enrich data insights. In parallel to this, the introduction of Swift GPI has also aided transparency, visibility and tracking of payments in real time.

Blockchain has been talked about by many as an emerging technology that could revolutionise the financial services industry and in particular, cross-border payments.

The recent pilot between Swift, Chainlink and Global Financial Institutions (Lloyds Banking Group participated in this), demonstrated that interoperability can be achieved between traditional and decentralised finance applications, that could unlock access to new infrastructure and business value [3].

Additional benefits of blockchain could also be unlocked from the immutable nature of the technology, the transparency created across the network as well as it's "always on" features. At its core though, the technology acts a security layer that establishes trust between members, where trust does not necessarily exist today.

This paper will directly explore how blockchain could be applied to enhance the cross-border payments journey in the following chapters.

LLOYDS BANK

Exploring cross-border payments

Earlier this year, Lloyds Bank began their exploration into blockchain to discover its potential to enhance the cross-border payments journey. A team was assembled to understand the journey, identify relevant problems and opportunities that blockchain could potentially address. The team consisted of payment experts, engineers and designers and followed an agile based methodology [4] over a three-month project window.

Before commencement, the team completed an evaluation of various blockchain infrastructure (Layer 1 technology) to understand the suitability for deploying enterprise software within a bank environment. Ethereum [5] was the obvious candidate given its large support network of developers, strong ecosystem for tooling as well as general purpose smart contracts.

With privacy being a critical characteristic for the bank, adoption of a permissioned network, Hyperledger Besu felt appropriate, which supports the public Mainnet and is Ethereum Virtual Machine (EVM) compatible. It also contains enterprise features such as transaction privacy, secure node permissioning on the network whilst underpinned by a Proof of Authority [6] consensus mechanism.

Whilst the engineering team began deployment, the business team commenced research, conducting qualitative interviews with internal Lloyds Bank colleagues, all of whom are involved with cross-border payments. The scope of work focussed solely on to business-to-business payments.

During these interviews a multitude of issues were uncovered, which are summarised below.

Outbound payment (Sending bank)	Payment initiation	■ Legacy Platforms ■ Data quality issues ■ Bespoke country requirements (e.g. Purpose Codes)
	Funds checking / KYC	■ Data capture issues for KYC
	Sanction checks / AML	■ Filtering Tools / Manual case checking ■ Local jurisdiction compliance ■ Sender bank must screen the beneficiary at the receiving bank
In-flight payment	FX & Routing	■ Time zones ■ Reliance on correspondent relationships ■ Tracking capabilities
Inbound payment [7] (Receiving bank)	Sanction checks / AML	■ Filtering Tools / Manual case checking ■ Local jurisdiction compliance
	Settlement	■ Finality of settlement ■ Legacy Platforms
	Reconciliation	■ Legacy Platforms

Use case identification

Following completion of the research and understand phase, the team settled on exploring Due Diligence, KYC and Sanctions through the concept of a digital identity. The interviews evidenced recurring friction points in cross-border payments, yet to be intimately explored, that could be solved with the application of blockchain.

Today, regulation requires all payments transactions to be screened to meet local jurisdiction requirements. This is a critical process to ensure banks comply with national and international regulations aimed at preventing money laundering, terrorist financing, and other illicit activities.

Failure to ensure payments do not breach sanctions can also lead to heavy penalties, with BNP Paribas agreeing to a record $9 billion settlement with US prosecutors in 2014 over allegations of sanctions violations against Sudan, Cuba and Iran [8]. It was also prevented from clearing certain transactions in US dollars for 2015 as additional punishment.

The process of screening a transaction is completed by all banks involved in the transaction. This means that a transaction will be screened as it leaves the issuing bank, and the process is repeated through the various intermediary banks and finally when the payment reaches the acquiring bank.

With banks operating inside their own walled gardens, it means that screening can take place multiple times during a transaction, leading to a huge duplication of effort and overall increase in the cost and time for a payment to settle. The issue is further compounded each time an intermediary is involved and subsequently required to screen both sending and receiving accounts on the inbound and outbound legs.

But what if banks could trust each other’s processes?

Application of Blockchain

Verifiable Credentials

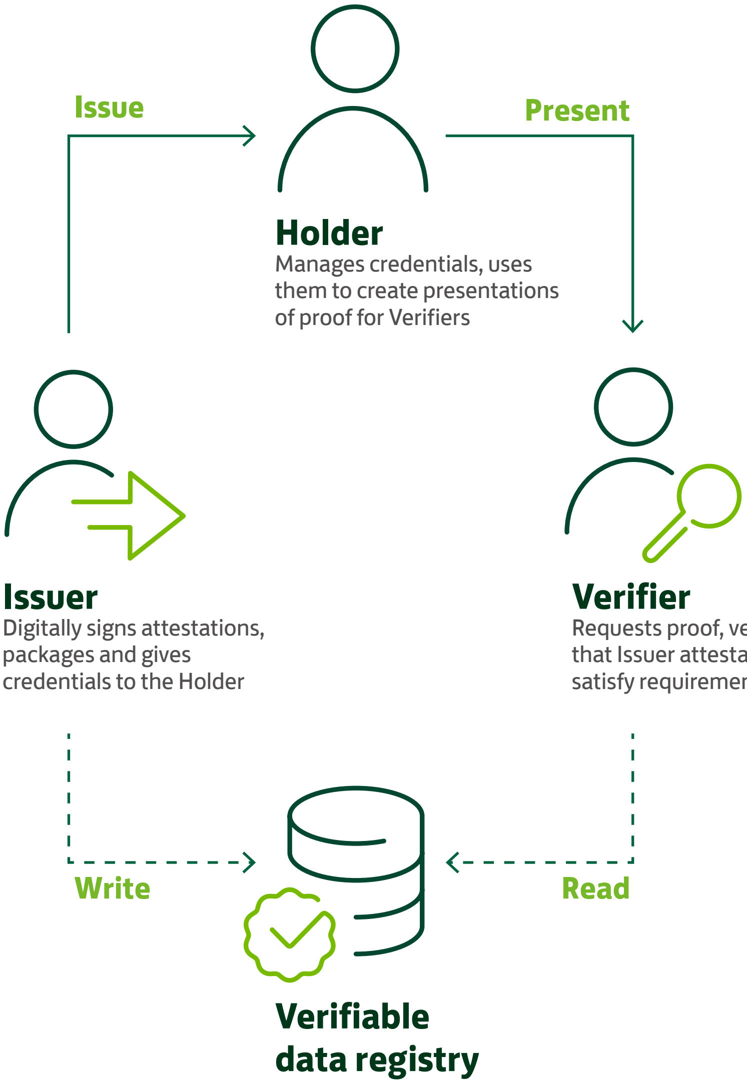
The concept of verifiable credentials has emerged as a digital alternative to the long-standing issues faced today with physical credentials (e.g. Passport, Driving Licence etc). Verifiable credentials are used to prove things about a subject and are fraud proof, fully auditable and instantly verifiable for authenticity.

A credential will typically consist of information related to identifying the subject of the credential (e.g. name, identification number), information related to specific attributes being asserted by the issuer (e.g. nationality, date of birth) as well as information related to the duration of the credential (e.g. validity period).

The team explored how this concept can be applied to a corporate identity and to do so, leveraged a recognised Web3 framework to test verifiable credentials for on-chain identity.

Overview

1. Verifiable Credentials are digital, cryptographically secured versions of both paper and digital credentials (e.g. Passport, Driving Licence etc)
2. The holder of a verifiable credential sits at the centre of a triangle of trust, that mediates between an issuer and a verifier
3. The issuer and holder trust each other, the holder trusts the verifier, and the verifier trusts the issuer


Issue
Present
Holder
Manages credentials, uses them to create presentations of proof for Verifiers
Issuer
Digitally signs attestations, packages and gives credentials to the Holder
Verifier
Requests proof, verifies that Issuer attestations satisfy requirements
Write
Read
Verifiable data registry

How could this work for Financial Services?

Issuance of Credentials

We propose introducing a permissioned network where only authorised issuers (e.g. Banks / Trusted KYC providers) can produce verifiable credentials. The credential is stored offline by a holder (Issuing Bank) until it's required to present to a verifier (Receiving Bank) via a smart contract.

Members will continue to complete their KYC and onboarding processes for corporates exactly as they do today. Now, in parallel to this, banks create and issue a credential based on a schema in a blockchain registry. The registry will store only the credential schemas and the list of approved issuers (e.g. Banks).

Issuers (e.g. Banks) will first register their own digital identity on the blockchain, as well as schemas for the credentials they plan to issue. The schemas define a set of claims that can be made about individuals or businesses. Issuers construct credentials based on these schemas, attesting to the value of each claim for a particular entity. They sign the credential with their own digital identity.

A key distinction though to the diagram above, is that we assume banks will act as custodians of digital credentials on behalf of customers I.e. They will not be directly issued to corporates.

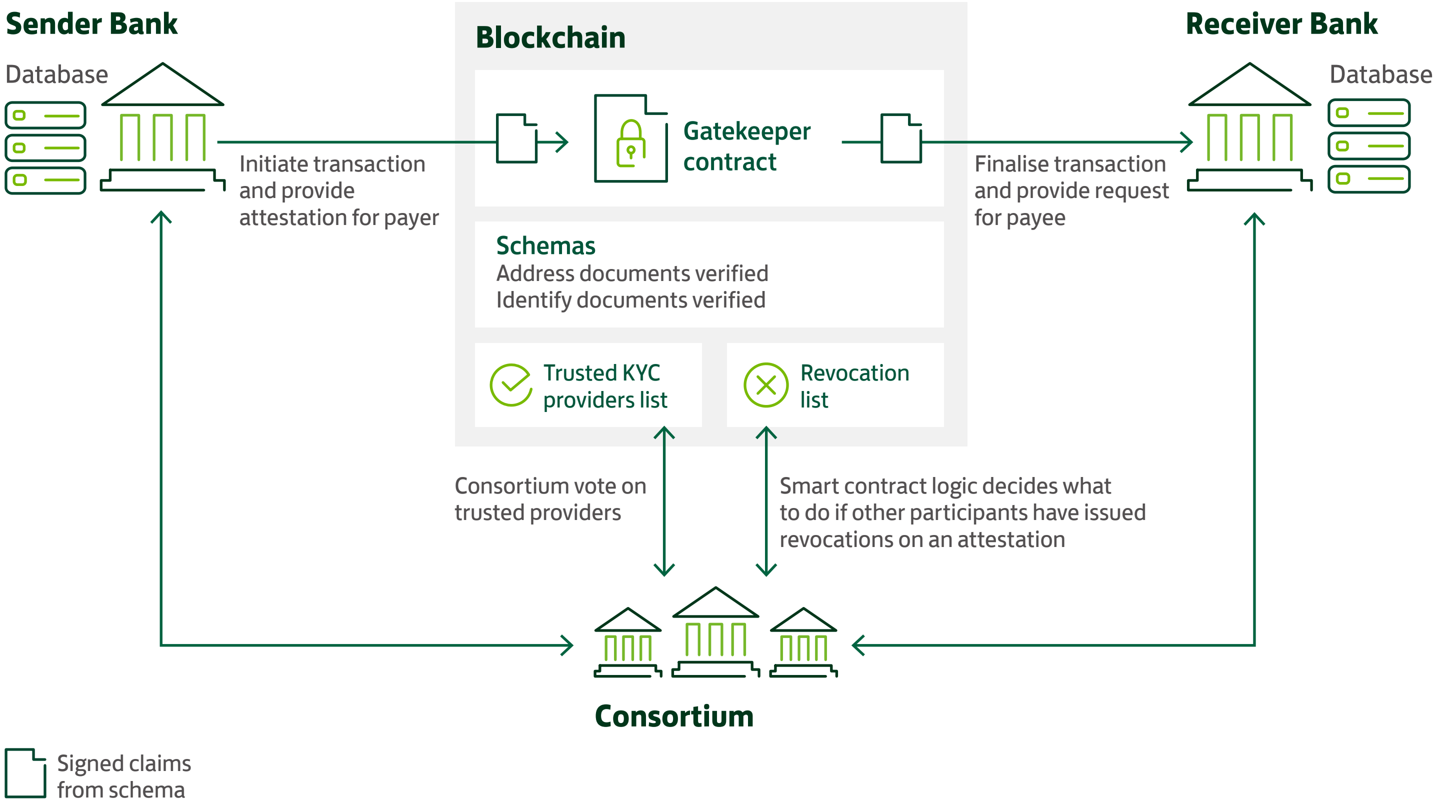
Contents of Credentials

The credential will include the identifier of the entity issuing it, that of its holder, the dates of its creation and expiry. The validity of the signature is cryptographically verifiable.

Each credential issued will have a verification key stored on the permissioned blockchain. Whilst the keys do not hold the credential data, or any personal information, they are used by permissioned members to verify credentials (e.g. attest to) involved in a transaction.

Credentials will in essence contain claims that certain evidential data has been verified by the Issuer. The data itself won't be recorded on the credential, but instead a hash of this data can be included for auditing purposes.

Banks store attestations about customers in their databases. Attestations can be from themselves or a trusted third-party KYC provider


Sender Bank
Database
Initiate transaction and provide attestation for payer
Blockchain
Gatekeeper contract
Schemas
Address documents verified
Identify documents verified
Trusted KYC providers list
Revocation list
Receiver Bank
Database
Finalise transaction and provide request for payee
Consortium vote on trusted providers
Smart contract logic decides what to do if other participants have issued revocations on an attestation
Consortium
Signed claims from schema

Verification of Credentials

When a customer initiates a payment, the bank will use the issued credentials to prove things about the customer's identity (e.g. They are whitelisted in a jurisdiction).

The smart contract will not process transactions from individuals without valid certification. This acts as a pre-requisite to transact, exactly as banks do today.

The verifier (e.g. Receiving Bank) will check that the credential is signed by a trusted entity and that the claims satisfy its own constraints to move a transaction forward.

The issuing bank will sign the attestation that matches against the customer's credentials. Synchronously, the recipient bank will provide an attestation about the receiver's credential, thus allowing the transaction to proceed. The process would be automatic and immediate unless issuers required additional manual checks, in which case the credential would be posted once all claims are checked, so that the transaction can complete.

The role of Oracles

When smart contracts require information to validate a credential on behalf of an entity, decentralised oracle systems [9] can stamp on-chain, information from off-chain databases. This essentially bridges the blockchain with events in the outside world.

Of course, one of the major constraints with sanctions screening for banks is maintaining local lists that are perpetually refreshed and updated. The creation of an oracle(s) to link information to the blockchain such as sanctioned countries and entities in a jurisdiction would greatly assist the screening process.

Credentials could therefore reference off-chain databases / registries containing a combination of existing bank data such as IBANs, Bank Account Numbers and Legal Identifier Codes (LEIs) [10]. So long as the chain is permissioned (running on a private network) and members have access to this level of information it could sit on chain.

If this were to be expanded in the future to a public network, proofs would likely need to be stored off chain through usage of zero knowledge proof (ZKP) [11], to allow a verifier to attest to the validity of real-world information whilst ensuring privacy.

Establishing a secure network

To maintain a consistent standard, we propose introducing a scheme that participants would co-create or sign up to (e.g. what would be written on-chain). This would mean commitment to agreed standards (globally) so that when credentials are issued on behalf of corporates, it provides confidence to fellow members that certain standards are being adhered to.

As this expands, the list of issuers on the network could be managed in a number of ways. One approach could be through a DAO [12] community, a list of approved institutions through a consortium, or alternatively, from a higher standard such as Central Banks and/or regulators.

Members of the network would be able to vote to revoke bad actors whether it be either the corporate's credential or even the issuing bank. This acts as an incentive for issuers to maintain a robust standard as without this, they cannot facilitate in transactions or be rewarded by providing attestations to wider transactions in the network.

To further bolster the veracity of the network, audit nodes could be introduced onto the network to review attestations and ensure reliability. This would involve transactions containing a hash of the evidential data backing a credential being attached to the credential itself. When auditors see that a transaction used a particular credential, they can request the evidential data from the issuer used to produce it. If the hash of the evidential data provided to the auditor doesn't match the hash of the evidential data in the transaction, the auditor would know that it has been tampered with since it was used.

Auditors would consequently be able to request access to credentials about corporates which would be in the form of off-chain KYC information by the issuing bank. However, evidential data would be retrospective of the event and reviewed offline.

What does this mean for cross-border payments?

The network establishes a composable trust model between members and challenges today's notion that banks must individually screen a transaction.

We see the real potential of this proposition being unlocked if wider network participants can become incentivised to provide attestations for credentials outside of their own direct involvement. To do so it will likely require a fee-based incentive model and some acceptance of liability.

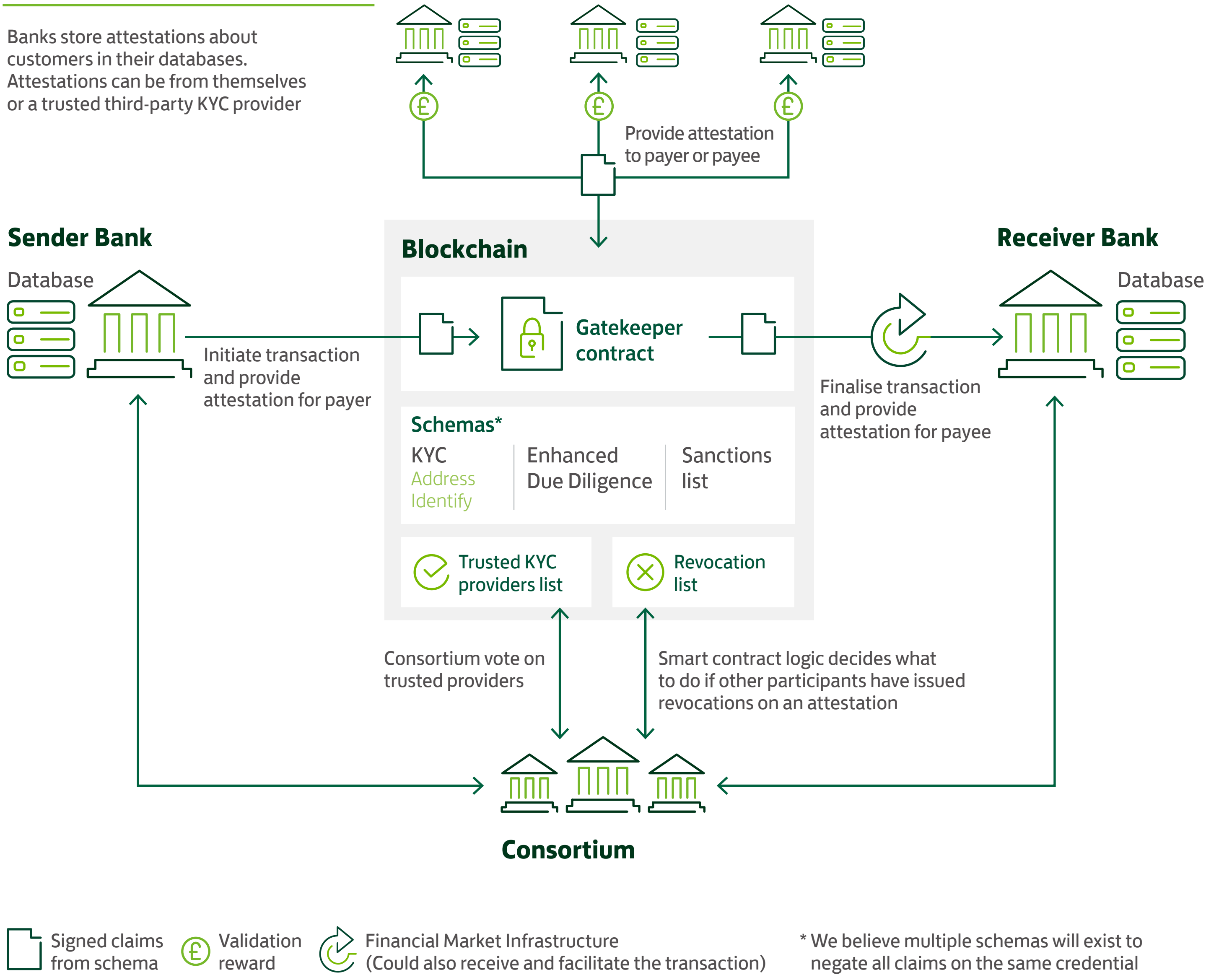
But with additional banks responding and attesting to credentials, the veracity of the credentials themselves will further strengthen. This in essence becomes a multi-party KYC, with members no longer relying on an attestation solely by an issuer.

Today, cross-border payments involve intermediary banks who are required to screen transactions prior to the payment reaching its final destination. Instead, intermediary banks could lean on other network member's attestations, thereby taking a significant level of cost and time out of the payment journey.

By leveraging a global network of banks, a multi-party KYC would reduce friction points that persist today with screening, particularly when transactions become trapped internationally in time zones.

If such a model were to be considered in future, further work will be required to identify and consider what legal and regulatory challenges exist (e.g. GDPR compliance and outsourcing). We would welcome views on this from any interested parties.

Banks store attestations about customers in their databases. Attestations can be from themselves or a trusted third-party KYC provider



Provide attestation to payer or payee
Sender Bank
Database
Initiate transaction and provide attestation for payer
Blockchain
Gatekeeper contract
Schemas*
KYC
Address
Identify
Enhanced Due Diligence
Sanctions list
Trusted KYC providers list
Revocation list
Receiver Bank
Database
Finalise transaction and provide attestation for payee
Consortium vote on trusted providers
Smart contract logic decides what to do if other participants have issued revocations on an attestation
Consortium
Signed claims from schema
Validation reward
Financial Market Infrastructure (Could also receive and facilitate the transaction)

* We believe multiple schemas will exist to negate all claims on the same credential

Conclusion

Verifiable credentials could be deployed to rapidly enhance the KYC, Due Diligence and Screening process for banking today.

Today's regulation requires Banks to complete full KYC and Due Diligence whilst screening all individual payments. In our outlined approach, network members would instead be able to lean on the wider network participants that have attested to a credential. This could reduce the level of sanctions screening checks required by intermediaries throughout the cross-border payment journey.

The use of blockchain facilitates and guarantees the exchange of the data of all its users, making it possible to establish relationships of trust between banks acting as issuers, holders and verifiers of credentials. The immutable nature of blockchain also provides trust that attestations have not been tampered with and are fully traceable / transparent across the network.

In a world where tokenisation and propositions like Fnality or the Regulated Liability Network continue to grow, this could become a natural complement to moving both data and money in one synchronous movement.

Definitions

Blockchain (Layer 1) – An underlying system in which a record of transactions are maintained across computers that are linked in a peer-to-peer network system.

Blockchain (Layer 2) – Any off-chain network, system, or technology built on top of a blockchain to help extend its capabilities.

Decentralised Autonomous Organisation (DAO) – An organisation managed in whole or in part by decentralised computer program, with voting and finances handled through a blockchain. In general terms, DAOs are member-owned communities without a centralised leadership.

Ethereum – Ethereum is an open source, decentralized blockchain with smart contract functionality.

Hashing – A mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length.

Know Your Customer (KYC) – Regulations in financial services that require institutions to verify the identity, suitability, and risks involved with maintaining a business relationship with a customer.

Oracle – Blockchain oracles are entities that connect blockchains to external systems, thereby enabling smart contracts to execute based upon inputs and outputs from the real world that are not on-chain.

Proof of Authority – A method of achieving consensus (agreement) that allows approved accounts, known as validators, to validate transactions and blocks. There is no incentive or reward mechanism, instead validators take turns to create the next block in a round robin based format.

Smart Contract – A computer program or a transaction protocol that is intended to automatically execute, control, or document events according to the terms of a specified contract or an agreement.

Verifiable Credentials – An open standard for digital credentials. They can represent information found in physical credentials, such as a passport, as well as new things that have no physical equivalent.

Contributors

Stephen Eddy
Blockchain Developer
Lloyds Bank

Sam Taylor
Blockchain Developer
Lloyds Bank

Sam Dermott
Payments, Partnership & Strategy
Lloyds Bank

Richard Beverley
Economic Crime Product Owner
Lloyds Bank

Ravi Shukla
Group Innovation
Lloyds Bank

1 Cross-border Payments | Bank of England

2 G20 Roadmap for Enhancing Cross-border Payments: Priority actions for achieving the G20 targets – Financial Stability Board (fsb.org)

3 Swift explores blockchain interoperability to remove friction from tokenised asset settlement

4 What is Agile? | Atlassian

5 Ethereum.org

6 Definition of Proof of Authority

7 Lloyds Bank research into cross-border payments

8 Fines for banks that breached US sanctions (refinitiv.com)

9 Decentralised Oracles Why Do Blockchains Need Oracles? (forbes.com)

10 Introducing the Legal Entity Identifier (LEI) – GLEIF

11 Definition of Zero Knowledge Proof

12 Definition of Decentralised Autonomous Organisations

Go online:
lloydsbank.com/financial-services

Speak to your
Relationship Manager

Please contact us if you would like this information in an alternative format such as Braille, large print or audio.

Lloyds Bank plc. Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England and Wales no. 2065. Telephone: 0207 626 1500. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority under registration number 119278.

Lloyds Banking Group is a financial services group that incorporates a number of brands including Lloyds Bank. More information on Lloyds Banking Group can be found at lloydsbankinggroup.com.

LLOYDS BANK