

Blockbill: An Electronic Bill of Lading System

Robert Blake
robert_blake@hotmail.co.uk
www.blockbill.co.uk
31 October 2024

Abstract. Bills of Lading are an essential part of international trade, but the existing paper Bill of Lading system incurs serious delays, costs and risks. Following the enactment of the UK's Electronic Trade Documents Act 2023 electronic Bills of Lading may now be viable, but existing solutions suffer from the inherent weaknesses of relying upon a trusted third party. The Liquid network, a Bitcoin sidechain, allows users to verifiably issue, transfer and destroy a unique blockchain token. This paper defines an open source protocol for using such a token as a data structure evidencing exclusive control of the Bill of Lading. Details of the token may then be endorsed onto a human-readable electronic copy of the Bill of Lading. Together these elements form a reliable electronic Bill of Lading system that is swift, inexpensive and secure.

1. Introduction

Bills of Lading are an essential part of international trade. However the existing paper Bill of Lading system is slow, costly and high risk for all parties involved.¹ A solution lies in electronic Bills of Lading. However adoption has been limited² whilst awaiting two key developments. Firstly, following the invention of Bitcoin and blockchain technology in 2008, a verifiably unique digital token may now be used to represent the Bill of Lading. And secondly, with the entry into force of the Electronic Trade Documents Act in 2023, parties are now assured that electronic Bills of Lading have the same legal effect as an equivalent paper Bill of Lading.

The Electronic Trade Documents Act

Around £1.4 trillion of international trade is conducted via the UK.³ 80% of Bills of Lading used in international trade are subject to English law and jurisdiction.⁴ Based upon proposals⁵ set out by the Law Commission, the Electronic Trade Documents Act 2023⁶ ('the Act') entered into force on 20 September 2023. Briefly, Section 1 of the Act specifies the paper trade documents, including Bills of Lading, to which the Act applies. Section 2 defines an electronic trade document and the requirements for a reliable electronic trade document system. Section 3 provides that an electronic trade document has the same effect in law as an equivalent paper trade document. And Section 4 sets out the requirements for conversion of a paper trade document to an electronic trade document and vice versa.

Increased Trade and Efficiency

The International Chamber of Commerce estimates the Act will reduce the time needed for processing documents by up to 75% and may generate £171 billion in efficiency savings from electronic Bills of Lading alone.⁷ They further predict electronic trade documents will result in a 35% business efficiency improvement and a 13% increase in international business for Small and Medium sized Enterprises.⁸ Major container shipping lines have together committed to converting to 50% electronic Bills of Lading by 2028 and 100% by 2030, with estimated savings of \$6.5 billion.⁹

Proposal

This paper proposes a permissionless, open source electronic Bill of Lading system using an established Bitcoin based blockchain, namely the Liquid network. Using this sidechain parties may issue a verifiably unique digital token. This token may act as a data structure evidencing exclusive control logically associated with a human-readable electronic copy of the Bill of Lading. Control of the unique token is equivalent to possession of the paper Bill of Lading. We may thereby greatly increase the speed of transfer of the Bill of Lading, decrease the cost of transfer, and reduce risk to Carriers, Insurers and Lenders.

Section 2 of this paper sets out the functions of Bills of Lading, their practical use and the problems inherent in the existing paper Bill of Lading system. Section 3 describes how blockchain technology may be used to solve these problems and the blockchain characteristics required to do so. Section 4 outlines the Liquid network, an established Bitcoin sidechain and how this may be used for our purposes. And Section 5 explains the procedure by which an electronic Bill of Lading may be verifiably issued, transferred, and destroyed.

2. The Paper Bill of Lading Problem

Importance

Bills of Lading are documents used in international trade, chiefly in the carriage of goods by sea, with three principal functions:

1. documenting the Contract of Carriage between the Shipper and the Carrier;
2. serving as a receipt for the cargo delivered to the Carrier; and
3. acting as a transferrable Document of Title entitling the bearer to take delivery of the cargo from the Carrier.¹⁰

An estimated 25 billion paper trade documents are generated and couriered around the world annually.¹¹ The shipping industry alone generates four billion paper trade documents per year.¹² Of these an estimated 45 million¹³ Bills of Lading are issued annually in the container trade with a further one million¹⁴ Bills of Lading in the bulk cargo trade.

In Practice

The Shipper delivers their cargo on board the Carrier's Vessel. In exchange the Carrier issues a receipt, named the Bill of Lading, to the Shipper stating the quantity and condition of the goods received on board. The terms and conditions of the Contract of Carriage between the cargo owner and the Carrier are printed on the reverse of the Bill of Lading.

The Bill of Lading, particularly in the bulk cargo trade, is often a negotiable bearer document traded by means of a separate contract of sale whilst the cargo is in transit. There may be a chain of contracts of sale and the Carrier is normally unaware of who is the rightful holder of the Bill of Lading. Upon arrival at the discharge port the Carrier is obliged to deliver the cargo to the bearer upon presentation of the Bill of Lading. Thereafter the spent Bill of Lading may be marked as 'accomplished' by the Carrier and ceases to have effect as a document of title.

Letters of Credit

A Buyer will often obtain finance to fund the purchase of the cargo. In order to secure their loan the Buyer's bank issues a Letter of Credit naming the Seller as beneficiary with payment conditional upon presentation of the Bill of Lading to the Buyer's bank. Each party in the chain of contracts of sale may have obtained similar finance, leading to a chain of Letters of Credit and banks through which the Bill of Lading must pass before it can be presented to the Carrier.

Delays and Risks

At each stage of this chain the Bill of Lading must be securely couriered by each party to the next and checked thoroughly. This incurs delays such that the Bill of Lading is normally not available at the discharge port.

Upon arrival at the discharge port the Charterer of the Vessel may order the Carrier to discharge the cargo to a party whom they understand to be lawfully entitled to the cargo without presentation of the Bill of Lading. If the Carrier misdelivers the goods to the wrong party, even acting in good faith, they are liable in conversion to the rightful holder of the Bill of Lading. Such liability can run into hundreds of millions of dollars. However, the Carrier is also under commercial pressure to expedite discharge of the cargo so their vessel may proceed on its next scheduled voyage, or face losing tens of thousands of dollars per day in operating expenses.

Letters of Indemnity

To deal with this dilemma the Carrier generally agrees to instead accept a 'Letter of Indemnity' from the Charterer promising to defend them and provide security against any losses or consequences arising as a result of discharging the cargo without presentation of the Bill of Lading. The Carrier may demand that the Receiver's bank countersign the Letter of Indemnity, though this is rarely provided.

In turn the Charterer may demand a Letter of Indemnity from the cargo Receiver and so on through the chain of contracts of sale. This creates a chain of Letters of Indemnity which must be in place before the cargo is finally ordered to be discharged.

Should there be a dispute as to the rightful holder of the Bill of Lading the Vessel may be arrested and held pending provision of security, running into tens of millions of dollars, before being released. However there is no guarantee that the issuer will honour their Letter of Indemnity. In discharging the cargo against a Letter of Indemnity the Carrier is therefore forced to accept the credit risk of the issuer.

Strictly, discharging the cargo against a Letter of Indemnity also invalidates the Carrier's insurance cover and the Carrier must rely upon their insurer providing discretionary cover.

Costs

Issuing and managing of paper Bills of Lading, Letters of Indemnity and other documents is estimated to cost upwards of 15% of the physical transportation costs.¹⁵ Despite this, paper Bills of Lading remain vulnerable to loss, theft and fraud.

Summary

Paper Bills of Lading are fraught with delay, costs and enormous risk for any party dealing with them, and particularly so for the Carrier.

3. The Blockchain Solution

Electronic copies

Why then do the parties not simply agree to accept an electronic copy of the Bill of Lading? The problem, of course, is that an electronic copy may be trivially duplicated. The party receiving the electronic copy of the Bill of Lading has no way to guarantee the sender has not sent a duplicate copy to another party, in effect 'double spending' the Bill of Lading.

Trusted third party model

One solution might be to rely on a trusted third party to operate a database, or 'centralised ledger', against which the true ownership of the electronic Bill of Lading may be checked. Such proprietary systems already exist, principally focussing on the container trade. Whilst such systems may work well enough, they still suffer from the inherent weaknesses of the trust based model:

1. All parties who deal with the Bill of Lading must subscribe to that same system.
2. Users must accept the risk that their transactions may not being accepted, or that details of their transactions may be obtained by a competitor, or that the system itself may be discontinued.
3. A rogue actor with access to a centralised database may easily alter it for their own benefit. Users rely entirely upon such rogue actors being properly vetted by the third party and excluded from the system.
4. Users are unlikely to have access to the proprietary software underpinning the system, let alone the centralised database or distributed ledger which holds the relevant data. Users must therefore rely entirely upon the word of the third party, or an auditor periodically granted access by that third party, for the integrity of the system.

Blockchain model

What is needed is an electronic system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.¹⁶

The Bitcoin network solves the electronic 'double spend' problem without reliance upon a trusted third party using a 'blockchain.' The blockchain contains a record of each and every transaction on the network assembled into a chain that is computationally infeasible to alter. Individual users operating decentralised 'nodes' each maintain a copy of this blockchain, in a so-called 'distributed ledger'. Each node is able to enforce the rules of the network and reject any transaction that attempts to 'double spend' a coin recorded on the blockchain as already having been spent.

Uniqueness

Whilst this takes us some of the way towards a solution, the commercial and legal value of the Bill of Lading is dependent upon its uniqueness. However a token on the Bitcoin blockchain is fungible. What we require is a unique token on a blockchain to represent the Bill of Lading. Users may then verify for themselves that the token is unique.

Standalone vs Existing Blockchain

Creating a standalone blockchain might be one solution. However, of the 86,000 blockchain projects launched after 2009, only 8% remained actively maintained by 2017¹⁷. Commercial parties must be assured that any blockchain they rely upon will remain operational. Using a well-established blockchain increases the likelihood that it will remain operational. A blockchain with 'open source' code is also more easily audited than one based on proprietary code.

Two Component Data Structure

Proprietary systems often attempt to place all the information otherwise stated in a paper Bill of Lading, including the voluminous terms and conditions of the Contract of Carriage, into the data structure itself. This requires all parties to use the same proprietary system or standard as well as generating a bloated data set. Large data requirements may mean fewer users run their own node and result in less, or no, independent verification of the blockchain. Many commercial parties also trade in jurisdictions where their counterparties and the local customs authorities may require a hard copy Bill of Lading and hence do not wish to use an integrated data structure.

Fortunately the Act allows greater flexibility in how information may be structured. Sections 2(1) and 2(2) of the Act together provide that an electronic trade document may be comprised of separate but linked elements: a paper trade document in electronic form, along with '*...other information with which it is logically associated that is also in electronic form*'. The Law Commission provides further guidance: 'logically associated' means electronically connected to, linked or otherwise cross-referenced to. This wording is expressly intended to enable the use of different models of electronic trade documents managements systems in line with the principle of technological neutrality.¹⁸ An electronic trade document may therefore consist of two components: the underlying data structure which makes it amenable to exclusive control, and a human-readable element which evidences rights and obligations.

For ease of adoption, any system should be familiar to those working in the shipping industry. The simplest way to achieve this is to use an electronic copy of the Bill of Lading, say a PDF, as the human-readable element, and a separate unique blockchain token as the underlying data structure. The two elements may then be logically associated simply by endorsing the electronic copy of the Bill of Lading with a statement that it is only valid with electronic control of a specified and unique blockchain token.

Regulatory Risk

Many alternative blockchain projects distribute tokens to their backers via a so-called 'pre-mine' in order to raise capital. The US Securities and Exchanges Commission views such projects as unregistered securities and continues to pursue court cases against firms involved with such blockchains¹⁹. For a commercial party this represents a risk that regulatory action may prevent their use of such blockchains. However Bitcoin is created via a predetermined schedule and is considered by US regulators to be a commodity.²⁰

4. Liquid

Sidechain

What is needed is a well-established, Bitcoin based, blockchain that allows users to issue a unique token. One such system is the Liquid network,²¹ a so-called Bitcoin sidechain, that is an independent blockchain which supports an automatic peg mechanism to the Bitcoin blockchain. The Liquid network has been in continuous operation since its launch on 10 October 2018 and presently handles over \$310 million of assets.²² The Liquid network uses code derived from the Bitcoin codebase and transactions are funded using L-BTC, an asset that is verifiably pegged 1:1 with BTC on the Bitcoin network.²³ The Liquid network software is open source and freely available for audit by any interested party.²⁴

Security

The Liquid network uses a Bitcoin-like 'Unspent Transaction Output (UTXO)' model. Each UTXO is secured with a cryptographic public-private key pair. The holder of the private key exclusively controls the UTXO. In order to transfer control of the UTXO the receiver provides the sender with their public key 'address'. The sender then creates a transaction and digitally signs it with their private key. Users manage their UTXOs, public key addresses and private keys, and create transactions using a software 'wallet'.²⁵

Signed transactions are broadcast to the Liquid network. Specialised nodes named 'functionaries' group these transactions into proposed blocks in exchange for transaction fees. Once 11-of-15 functionaries independently validate the proposed block it is added to the blockchain.²⁶ Thereafter exclusive control of the UTXO has passed to the receiver and the transaction may not be cancelled or altered.

Verification

A distributed network of nodes each maintain a copy of the entire blockchain. Each node independently verifies the integrity of each and every block. Any block or transaction which fails to adhere to the networks' consensus rules is rejected. Any party may freely operate a node in order to validate transactions and view any information on the blockchain.²⁷

Issued Assets

Users of the Liquid network may issue their own tokens, named 'Issued Assets'. Additional information such as the amount to be issued is added to a regular transaction input in order to create the Issued Asset. A unique Issued Asset may be created and used as the underlying data structure of the electronic Bill of Lading. Anyone with knowledge of the issuance transaction may easily verify the uniqueness of that Issued Asset.

Confidential Transactions

Distributed ledgers allow any user to view the amounts transferred in a transaction. Data analysis firms may be able to identify users by analysing these transactions. For a commercial party this represents a risk that competitors may be able to obtain information on their trading activities that they would prefer to remain confidential. Users of the Liquid network may choose to further encrypt their transactions using the 'Confidential Transactions' feature²⁸. Whilst the addresses of the transaction sender and receiver remain visible, the asset type and the amounts are hidden. Users may provide the cryptographic 'blinding key' to auditors and other third parties at their discretion to allow them to view these confidential transactions.

Settlement Interval

Transactions on the Bitcoin network are considered to be irreversible after one hour. That is considerably faster than the several days often required for the couriering of a paper Bill of Lading or final settlement via SWIFT. Nonetheless commercial parties may still consider it advantageous to have electronic Bill of Lading transactions confirmed at an even shorter interval. The Liquid network offers users a consistent one minute block interval, with transaction finality after two blocks.²⁹ This may enable traders to engage in high frequency trading of cargo in transit and to take advantage of short-lived arbitrage opportunities.

Transaction Fees

The reduced interval between blocks allows a greater volume of transactions to be processed in a given timeframe. Liquid network transaction fees are therefore extremely low. At the time of writing transaction fees are around 15 cents.

Summary

Together these features provide us with a blockchain solution to the paper Bills of Lading problem that is swift, inexpensive and secure.

5. Protocol Structure

Who should issue the electronic Bill of Lading?

The greatest liability in the handling of the Bill of Lading attaches to the Carrier. The Carrier therefore typically controls the issue and cancellation of paper Bill of Ladings. The Carrier should similarly control the conversion of the paper Bill of Lading into an electronic Bill of Lading and vice versa. For convenience, let us begin with a paper Bill of Lading issued and signed by the Vessel's Master as normal.

Issuing an Asset

The minimum amount of an Issued Asset that can be issued or transacted on the Liquid blockchain is 0.00000001.³⁰ In order to guarantee the uniqueness of the Issued Asset the amount issued must therefore be exactly 0.00000001.

When issuing assets on the Liquid blockchain users have the option to create a reissuance token. The reissuance token allows the holder to issue further copies of the corresponding Issued Asset. If a reissuance token has been issued the parties cannot be sure that further copies of the Issued Asset have not been, or will not be, issued. The number of reissuance tokens issued must therefore be zero.

An issuer may use the Confidential Transaction feature of the Liquid blockchain and 'blind' the issuance transaction. However other parties must then be provided with the issuance blinding key if they wish to independently verify the amount issued. Commercial parties are primarily concerned with easy verification of the uniqueness of the Issued Asset. Blinding the initial issuance transaction and then providing the issuance blinding key to a party adds an unnecessary step in the verification process. The issuance transaction should therefore not normally be blinded. If, however, the issuer does wish to blind the issuance transaction, they may also wish to endorse the blinding key on the face of the electronic copy of Bill of Lading for the convenience of other interested parties.

The issuing process returns a unique asset ID and transaction ID to the Carrier. The unique asset is stored in the Carrier's wallet. The Issued Asset now forms the data structure element of the electronic Bill of Lading.

Endorse

Blockchain explorers typically analyse the entire chain of transactions recorded on the blockchain in order to construct an address and balance mapping database. This database may then be queried to show what balances are spendable from a given address. This requires the user to rely upon a blockchain explorer maintained by a third party. However the issuance transaction already contains the amount issued as well as whether or not a reissuance token exists. Anyone with knowledge of the issuance transaction may therefore, without querying a blockchain explorer, easily verify an asset is unique and that no reissuance token has been issued. The issuance transaction ID should therefore be endorsed on the face of the electronic copy of the Bill of Lading in addition to the Issued Asset ID.

Section 4 of the Act allows for the change of form from a paper trade document to an electronic trade document, and vice versa. Where a document is converted the old document ceases to have effect and the rights and liabilities relating to the document are transferred to its new form. Such conversion is only valid if a statement to that effect is included in the document in its new form. The endorsed electronic copy of the Bill of Lading should therefore state on its face that it is only valid with electronic control of the corresponding Liquid blockchain Issued Asset.

In order to avoid ambiguity the Carrier should include the date when the paper Bill of Lading is converted to an electronic Bill of Lading in addition to the statement required under section 4 of the Act. A statement such as the following should therefore be endorsed on the face of the paper Bill of Lading as it is converted to an electronic Bill of Lading:

“This paper Bill of Lading was converted to an electronic Bill of Lading on [date] in accordance with the England & Wales Electronic Trade Documents Act 2023 and is valid only with electronic control of Liquid blockchain Issued Asset ID [Issued Asset ID] issued in transaction ID [issuance transaction ID].

The endorsed electronic copy of the Bill of Lading, now forms the human-readable element of the electronic Bill of Lading. The paper Bill of Lading ceases to have effect at this time. It is nonetheless prudent to have any remaining paper copies marked as ‘void’.

SHA-256 Hash

The unique Issued Asset forming the data structure element is protected from unauthorised alteration by its inclusion in the Liquid blockchain. However parties must also be assured that the human-readable element, that is the electronic copy of the Bill of Lading, has not been altered. A simple way to achieve this is using a hashing algorithm. Hashing the file returns a unique string of characters which change if the data is altered in any way. A SHA-256 hashing algorithm is suitable for data integrity against attack. Once the details of the Issued Asset have been endorsed onto the face of the Bill of Lading the SHA-256 hash of the electronic copy should be noted by the Carrier and may be transmitted separately to any interested party. If the hash value of an electronic copy does not match the original value it will immediately be apparent that it has been altered.

Verify Asset

The human-readable electronic copy of the Bill of Lading may then be circulated to, and viewed by, any interested party as normal. Anyone with access to the Liquid blockchain may view the issuance transaction and easily verify the uniqueness of the Issued Asset. Any asset amounts greater than 0.00000001, reissuances, or the existence of reissuance tokens are immediately apparent.

Transfer Control

The Carrier may now transfer the Issued Asset to the Shipper. The electronic Bill of Lading may then be traded as normal whilst the cargo is en route to the discharge port. To transfer the Issued Asset the receiver first provides the sender with their public key address. The sender then creates a transaction on the Liquid blockchain and signs with their private key. After two blocks the transaction is final and exclusive control of the Issued Asset is transferred to the receiver.

Prove Control

Prospective Buyers may wish to have the Seller demonstrate control of the Issued Asset before entering into a contract with them. The Issued Asset is associated with a public key address. The person with control of that address may cryptographically sign a message using their corresponding private key in order to demonstrate control of that address.³¹

Whilst this demonstrates the Seller has control of the public key address we must also be sure the Seller had control of the Issued Asset itself at the time the message was sent. The message itself is not entered into a block and is not timestamped, however the transaction by which the Issued Asset was sent to the public key address is. By including this information in the body of the message we can be sure the message was signed after this incoming transaction, and that the Issued Asset was under the control of the Seller.

For ease of verification the message should also include the identity of the person claiming electronic control of the Issued Asset.

Verify Control

Anyone with access to the Liquid blockchain may easily verify that the message and address match the cryptographic signature.

Destroy Asset

Following arrival at the discharge port either the cargo Receiver or their bank may surrender, by a transaction on the Liquid blockchain, the Issued Asset directly to the Carrier in exchange for discharge of the cargo on board the Vessel. Upon completion of discharge of the cargo the Carrier may wish to endorse the human-readable electronic copy of the Bill of Lading as 'accomplished' in accordance with normal practice.

The Act does not require destruction of the electronic Bill of Lading. And, with the Issued Asset now under their control, it is not strictly necessary for the Carrier to destroy the data structure element. Nonetheless it is prudent to do so in order to eliminate any possibility of the Carrier accidentally transferring that Issued Asset to another party. Issued Assets on the Liquid blockchain may be destroyed³² by any person with control of the private key securing that asset.

Change of Form

Many commercial parties trade in jurisdictions which do not yet recognise electronic Bills of Lading, or with counterparties who would prefer to use a paper Bill of Lading. It may therefore be necessary to convert an electronic Bill of Lading back to a paper Bill of Lading.

It is not unusual for a Consignee to request a single paper Bill of Lading be split into separate Bills of Lading representing multiple cargo parcels. In these circumstances the Consignee surrenders the original Bill of Lading to the Carrier who controls the issuance of the split Bills of Lading. Similarly, and since in any event the Carrier must be made aware of the change of form, the Carrier should control any change of form from an electronic to a paper Bill of Lading and vice versa.

The Consignee requesting the conversion to a paper Bill of Lading should first surrender the Issued Asset directly to the Carrier.

Under Section 4 of the Act such conversion is only valid if a statement to that effect is included in the document in its new form. Section 4 of the Act does not require the underlying data structure to be destroyed when converting from an electronic trade document to a paper trade document. Nonetheless, again, it is prudent to destroy the Issued Asset at this time.

A statement such as the following should therefore be endorsed on the face of the electronic copy of the Bill of Lading when it is converted to a paper Bill of Lading:

“This electronic Bill of Lading was converted back to a paper Bill of Lading on [date] in accordance with the Electronic Trade Documents Act 2023 by the electronic destruction of Liquid blockchain Issued Asset ID [Issued Asset ID] in transaction ID [destruction transaction ID]”

The endorsed paper Bill of Lading may then simply be printed by the Carrier and despatched to the Consignee as normal.

Verify Destroyed

By endorsing the destruction transaction ID onto the face of the paper Bill of Lading any party with access to the Liquid blockchain may easily verify that the Issued Asset has, in fact, been destroyed.

6. Conclusion

This paper has proposed a permissionless, open source electronic Bill of Lading system using the Liquid network. A verifiably unique Issued Asset forms a data structure, details of which are endorsed onto the face of a human-readable electronic copy of the Bill of Lading. Control of the Issued Asset is equivalent to possession of the paper Bill of Lading. Users may then transfer control of the electronic Bill of Lading in minutes, at the cost of a few cents, and virtually eliminate the risk of misdelivery claims. The protocol is recapped below.

Protocol Summary

- Issue:** The Carrier has a paper Bill of Lading issued and signed as normal.
The Carrier issues a unique Issued Asset on the Liquid blockchain forming the data structure element of the electronic Bill of Lading.
- Endorse:** The Carrier has an electronic copy of the Bill of Lading endorsed with the Issued Asset ID and the corresponding issuance ID. This forms the human-readable element of the Bill of Lading.
The Carrier notes the SHA-256 hash of the electronic copy.
The Carrier has any unendorsed paper copies of the Bill of Lading marked as ‘void’.
The electronic copy of the Bill of Lading may then be circulated to any party.
- Verify Asset:** Any party may verify the uniqueness of the Issued Asset.
- Transfer Control:** The Carrier transfers the Issued Asset to the Shipper. Consignees may then trade the cargo en route as normal. Control of the Issued Asset is transferred via a transaction on the Liquid blockchain.

- Prove Control:** Sellers may demonstrate their control of the Issued Asset by cryptographically signing a message identifying themselves and including the incoming transaction by which they received the Issued Asset.
- Verify Control:** Any party may verify the message and signature match.
- Destroy Asset:** Upon arrival at the discharge port the Receiver with control of the Issued Asset may create a transaction and send it directly to the Carrier. Thereafter the Carrier may order the Master to deliver the cargo to the Receiver. Having completed discharge of the cargo the Carrier may destroy the Issued Asset.
- Change of Form:** If a party requires the Bill of Lading to be changed to a paper form the Issued Asset should first be transferred to the Carrier. The Carrier may then destroy the Issued Asset and endorse the paper Bill of Lading with the destruction transaction ID. The paper Bill of Lading may then be despatched as normal. Any party may verify the destruction of the Issued Asset.

Reliable System

Section 2(2) of the Act sets out the requirements for a reliable electronic trade document system. The protocol proposed in this paper identifies the electronic Bill of Lading using the unique Issued Asset. The Issued Asset is protected against unauthorised alteration by its inclusion in the Liquid blockchain. The electronic copy of the Bill of Lading is protected against unauthorised alteration using a SHA-256 hash check. The Issued Asset is secured by a cryptographic private key such that it is not possible for more than one person to exercise control of the electronic Bill of Lading at any one time. The person with control of the Issued Asset may demonstrate their control by cryptographically signing a message identifying themselves. Transfer of the electronic Bill of Lading has the effect to deprive the sender of their control. Accordingly this protocol satisfies the requirements of Section 2(2) of the Act.

Further Development

Whilst this protocol is designed to solve the paper Bill of Lading problem it may similarly be used for the electronic transfer of any unique trade document such as those listed in Section 1(2) of the Act.

The Liquid network also allows users to engage in so-called 'atomic swaps' whereby L-BTC or USDt, a 1:1 pegged USD asset, and an Issued Asset may be exchanged directly in the same transaction, eliminating counterparty risk or the need for escrow or credit arrangements.

References

- ¹ 'Legal Briefing, Electronic Bills of Lading', UK P&I Cub, May 2017 >> https://www.ukpandi.com/-/media/files/imports/13108/publications/28140---legal_briefing_e_bill_of_lading_web.pdf
- ² As of end 2021, only 1.2% of Bills of Lading were in electronic form - 'Disruption and the case for digital standards', Digital Container Shipping Association, 23 May 2023 >> <https://www.dcsa.org/newsroom/disruption-and-the-case-for-digital-standards>
- ³ House of Lords Debates on the Electronic Trade Documents Bill, 7 November 2022, Hansard, Col.146GC >> [https://hansard.parliament.uk/lords/2022-11-07/debates/EFDEB437-4656-42AA-B3FF-0531B0DFA9BB/ElectronicTradeDocumentsBill\(HL\)](https://hansard.parliament.uk/lords/2022-11-07/debates/EFDEB437-4656-42AA-B3FF-0531B0DFA9BB/ElectronicTradeDocumentsBill(HL))
- ⁴ Ibid., Col.151GC
- ⁵ Electronic Trade Documents Report and Bill, Law Commission, 15 March 2022 >> <https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2022/03/Electronic-Trade-Documents-final-report-ACCESSIBLE-1.pdf>
- ⁶ Electronic Trade Documents Act 2023 >> <https://www.legislation.gov.uk/ukpga/2023/38/contents/enacted>
- ⁷ 'Creating a Modern Digital Trade Ecosystem – the economic case to reform UK law', International Chamber of Commerce, 2021 >> https://www.wto.org/english/tratop_e/msmes_e/iccuk_240621.pdf
- ⁸ Ibid.
- ⁹ 'DCSA member carriers commit to fully standardised electronic bill of lading by 2030', Digital Container Shipping Association, 15 February 2023 >> <https://www.dcsa.org/newsroom/dcsas-member-carriers-commit-to-a-fully-standardised-electronic-bill-of-lading-by-2030>
- ¹⁰ 'Guide to Bills of Lading', West of England P&I Club, March 2018 >> https://www.westpandi.com/getattachment/907f94bf-b7dd-469e-913f-4baae23fca1d/p-i_guide_bills_of_lading_1_2pp_v2_lr.pdf
- ¹¹ House of Lords Debates on the Electronic Trade Documents Bill, 20 February 2023, Hansard >> [https://hansard.parliament.uk/lords/2023-02-20/debates/CEA7D90D-DFD5-491F-A202-AA06C75714BA/ElectronicTradeDocumentsBill\(HL\)](https://hansard.parliament.uk/lords/2023-02-20/debates/CEA7D90D-DFD5-491F-A202-AA06C75714BA/ElectronicTradeDocumentsBill(HL))
- ¹² House of Lords Debates on the Electronic Trade Documents Bill, 7 November 2022, Hansard >> [https://hansard.parliament.uk/lords/2022-11-07/debates/EFDEB437-4656-42AA-B3FF-0531B0DFA9BB/ElectronicTradeDocumentsBill\(HL\)](https://hansard.parliament.uk/lords/2022-11-07/debates/EFDEB437-4656-42AA-B3FF-0531B0DFA9BB/ElectronicTradeDocumentsBill(HL))
- ¹³ 'Disruption and the case for digital standards', Digital Container Shipping Association, 23 May 2023 >> <https://www.dcsa.org/newsroom/disruption-and-the-case-for-digital-standards>
- ¹⁴ 'Complete Guide to electronic Bills of Lading for the bulk trades', The Future of International Trade Alliance >> <https://www.fit-alliance.org/post/complete-guide-to-electronic-bill-of-lading-adoption-for-the-bulk-trades>
- ¹⁵ 'Legal Briefing, Electronic Bills of Lading', UK P&I Cub, May 2017 >> https://www.ukpandi.com/-/media/files/imports/13108/publications/28140---legal_briefing_e_bill_of_lading_web.pdf
- ¹⁶ See the Bitcoin whitepaper, 'Bitcoin: A Peer-to-Peer Electronic Cash System', 31 October 2008 >> <https://bitcoin.org/bitcoin.pdf>
- ¹⁷ 'The Evolution of Blockchain Technology', Deloitte Insights, 6 November 2017 >> <https://www2.deloitte.com/us/en/insights/industry/financial-services/evolution-of-blockchain-github-platform.html>
- ¹⁸ 'Electronic Trade Documents: Report and Bill', Law Commission, 15 March 2022, see Recommendation 9, paras.6.24-6.25, 6.30. Note Clause 1(3) of the Draft Bill was enacted as Section 2(2) >> <https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2022/03/Electronic-Trade-Documents-final-report-ACCESSIBLE-1.pdf>
- ¹⁹ 'LBRY, Winding Down, Drops Appeal of Crypto Ruling for SEC', Bloomberg Law, 23 October 2023 >> <https://news.bloomberglaw.com/litigation/lbry-winding-down-drops-appeal-of-crypto-ruling-favoring-sec>
- ²⁰ 'What is a Bitcoin Futures ETF', US Commodity Futures Trading Commission >> <https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/BitcoinFuturesETF.html>
- ²¹ See the Liquid whitepaper, 'Liquid: A Bitcoin sidechain', 22 May 2020 >> <https://blockstream.com/assets/downloads/pdf/liquid-whitepaper.pdf>

- ²² As of 31 October 24, see L-BTC >> <https://blockstream.info/liquid/asset/6f0279e9ed041c3d710a9f57d0c02928416460c4b722ae3457a11eec381c526d> and USDt >> <https://blockstream.info/liquid/asset/ce091c998b83c78bb71a632313ba3760f1763d9cfcffae02258ffa9865a37bd2>
- ²³ ‘What are Liquid assets?’, Blockstream >> <https://help.blockstream.com/hc/en-us/articles/900001543146>
- ²⁴ You can audit the code yourself here >> <https://github.com/ElementsProject/elements/releases>
- ²⁵ Compatible wallets include >> <https://elementsproject.org/> and <https://blockstream.com/green/>
- ²⁶ ‘What is a Liquid network functionary?’, Blockstream >> <https://help.blockstream.com/hc/en-us/articles/900003264706-What-is-a-Liquid-Network-functionary>
- ²⁷ You can follow these instructions to run your own node >> <https://help.blockstream.com/hc/en-us/articles/900002026026-How-do-I-set-up-a-Liquid-node>
- ²⁸ ‘Confidential Transactions’, Elements Project >> <https://elementsproject.org/features/confidential-transactions>
- ²⁹ ‘What is the transaction capacity of Liquid?’, Blockstream >> <https://help.blockstream.com/hc/en-us/articles/900001390903-What-is-the-transaction-capacity-of-Liquid>
- ³⁰ ‘Issuing your own assets’, Elements Project >> <https://elementsproject.org/elements-code-tutorial/issuing-assets>
- ³¹ Note that in order to sign a message the address must be in a Pay-to-Public-Key-Hash (P2PKH) format. The underlying script of a Pay-to-Script-Hash (P2SH) or a Bech32 (Segwit) format segregated witness address has a private key, but the address itself does not, and the message therefore cannot be verified.
- ³² Strictly, the asset remains part of the Liquid blockchain but is rendered ‘unspendable’ using the OP_RETURN script opcode. Thereafter it is impossible for the asset to be transferred to another party even with possession of the associated private key.