Primer on the DLPC: A Standard for Payment Commitments on the Blockchain

Authors: Rebecca Liao, Reid Monroe-Sheridan

Introduction

The painful and wide-ranging impact of supply chain disruptions over the past two years have brought new attention to the considerable complexity of global supply chains. Surprisingly, these increasingly complicated and sophisticated supply chain arrangements often rely on manual and paper-heavy processes to manage their complex underlying transactions. Recognizing an opportunity to improve these systems, the industry has looked for years to blockchain technology as a potential solution to the inefficiency, opacity, and expense of running a modern supply chain.

2019 marked a significant milestone in this effort. That year, a consortium comprised of the Banker's Association for Finance and Trade (BAFT), the largest trade association for transaction banking, 18 of the largest international commercial banks, and several technology companies (Skuchain[1], R3, Trade IX, we.trade, and CGI) created the Distributed Ledger Payment Commitment, or DLPC. The DLPC is a digital asset in the form of a legally binding payment commitment. It contains 13 simple data fields with information about the underlying transaction and is compatible with any blockchain protocol. In legal terms, it is essentially an electronic negotiable (or e-negotiable) promissory note that exists on the blockchain. Smart contracts and additional documentation can be attached to any DLPC to make it part of a financial flow.

As part of the DLPC project, BAFT has made available business best practices explaining the business and financial processes to be used with the DLPC as well as the instrument's legal backing. BAFT has also published technical best practices with specifications for the format of the DLPC and requirements for the systems in which it is used.

As a payment commitment, the DLPC is meant to be an eminently flexible instrument. To date, it has been used to replace guarantees, irrevocable payment undertakings and purchase orders in live supply chain transactions. In its simplest form, it allows banks to more easily track inter-bank obligations and corporate treasury departments to automate payments without direct integration with bank partners. However, the instrument's simplicity and flexibility provide the potential for a much greater range of applications.

The DLPC Legal Framework

Much of the DLPC's utility comes from its legal status as an electronic analog to a negotiable note. In basic terms, the holder of a negotiable note benefits from various protections that are unavailable to holders of non-negotiable instruments. Most importantly, it is generally faster and easier for the holder of a negotiable note to bring an enforcement claim against the issuer, with

---

[1] Rebecca Liao is Co-Founder, Advisor and former COO at Skuchain. Reid Monroe-Sheridan is Japan Advisor at Skuchain.

substantially less risk of the issuer successfully contesting the payment obligation or the amount owed. As a result, a negotiable note can typically be sold to a third party for a higher price than a non-negotiable note with identical terms. This allows the holder of a negotiable note to accelerate the receipt of cash and reduce counterparty risk by, for example, selling the note before its maturity date to a bank at a relatively small discount to the principal amount of the note.

The law governing these negotiable instruments is the conceptual foundation for the DLPC's legal structure. BAFT's DLPC best practices currently suggest that the DLPC will be governed by Delaware law because Delaware has been a leader in explicitly acknowledging the validity of e-negotiable instruments. Since BAFT reviewed appropriate legal frameworks for the DLPC, several countries have revised their laws to explicitly recognize e-negotiable instruments, and those countries may also provide suitable governing law for the DLPC depending on the needs of the transacting parties. The increasing international recognition of e-negotiable instruments is discussed in more detail below, but the Delaware law framework discussed in the DLPC business best practices merits particular attention.

Under Delaware law, the requirements for a payment commitment to be a negotiable instrument are set forth in the state's Uniform Commercial Code (UCC). In essence, the commitment must be an unconditional promise to pay some fixed amount of money on demand or at some point in the future. The commitment may include only a few other limited terms, and the inclusion of any impermissible terms will cause the commitment to fail to qualify for status as a negotiable instrument under the UCC.

Although the UCC's requirements are clear for paper-based payment commitments, digitizing these instruments is a challenging exercise. For example, negotiable notes must have a single, definite "holder" who will benefit from the legal protections of holding a negotiable instrument. Determining the holder is usually easy with a signed paper note: the holder is typically the person who has possession of the original, signed note.

In contrast, a digital note can be transmitted, in identical form, to many people simultaneously with the click of a button. In that case, who is the holder of the original note? Is there an original note at all? The Delaware Uniform Electronic Transactions Act (UETA) provides a framework for answering these questions and applying the UCC to electronic transactions. BAFT used this framework to propose a comprehensive solution for e-negotiable notes in the DLPC.

Under the UETA, a digital instrument that would otherwise fulfill the requirements to be a negotiable note will become a "transferable record" with the issuer's express agreement. A transferable record is basically an e-negotiable note, governed by the UETA, and the person deemed to have "control" over the transferable record will benefit from the UCC's protections as if that person were a holder of an original, physical paper version of the note.

Under the UETA, a person is deemed to have control over a transferable record if certain requirements are met. First, there must be a "single authoritative copy of the transferable record" that is "unique" and "identifiable" and may not be altered except as permitted by the UETA. Second, the authoritative copy must have been issued or transferred to the person claiming control over the record. There are additional requirements, including that the person controlling the record must have authority to prevent further changes to the authoritative copy, that the authoritative copy must be readily distinguishable from any duplicates, and that authorized modifications of the authoritative copy must be readily distinguishable from unauthorized modifications.

The blockchain's immutability, tamper-resistance, and verifiability (which are described below in more detail) are ideal characteristics for a system implementing solutions that meet the UETA's transferable record requirements. BAFT's best practices combine these characteristics with additional business and technical guidelines to help ensure satisfaction of the UETA's requirements.

The best practices specify the 13 data fields that should comprise the DLPC, as well as the data format for each field and permitted values. In addition to promoting cross-network compatibility, these standardized criteria help to ensure that the DLPC meets the UCC's strict limitations on terms that may be included in negotiable notes, which is required in this context for treatment as a transferable record under the UETA.

The DLPC best practices also include rules for the DLPC lifecycle. Each DLPC has four possible statuses (represented by the "Commitment State" field of the DLPC). The status may be "initiated," "contingent," "effective" or "discharged." When the DLPC has "contingent" status, the instrument is legally binding but its payment commitment is conditional in one or more respects. Once the DLPC's status becomes "effective," it represents an unconditional promise to pay and assumes the status of a transferable record. Contingent and effective DLPCs may only be modified in compliance with precise rules described in the best practices. These restrictions on permitted modifications promote compliance with the UETA's requirements regarding who may create, control and change a transferable record.

Finally, the DLPC best practices take advantage of Delaware's flexible approach to contracts. The best practices include standard contracting terms for parties involved in any DLPC transaction. These terms aim to ensure that the DLPC is treated as a transferable record under the UETA and clarify that the person identified in the "Committer" field of the DLPC will be treated as the person who controls the record (i.e., the holder of the digital note). The contract terms also provide that Delaware law will apply to DLPC transactions and disputes will be submitted to resolution in Delaware courts.

A Technical Overview of the DLPC

The DLPC is specifically designed to leverage the unique characteristics of blockchain systems. A blockchain is an immutable, distributed ledger that allows parties to transact securely without a trusted intermediary. Accordingly, once a DLPC is originated on a blockchain, it can be used as a secure payment commitment and leveraged as the basis for financing, all without independent verification from a third party. The characteristics of blockchains described below make them a particularly attractive platform for an instrument like the DLPC.

- **Security**: A blockchain network is a distributed system without a single point of failure. The mechanism by which it allows transactions to be settled is through consensus among multiple participants in the network. Such consensus is usually achieved through algorithmic means, supplemented by security checks—not through substantive agreement on the terms of each transaction. Different blockchain protocols have slightly different technical designs, but they all have these core features. To date, various applications built around blockchains, such as wallets, exchanges and custodians have been subject to successful cyberattacks, but never blockchains themselves.

- **Immutability**: Once a transaction has been settled on a blockchain, it will become part of a "block" of transactions settled around the same time, and these blocks will form a chain. More blocks may be added to the chain in the future, but the chain may not otherwise change. Therefore, if a transaction was submitted by mistake, an additional transaction can act as a corrective to the original mistaken transaction, but the original transaction is not overwritten within the blockchain; it remains part of the chain. This immutability is what allows participants in a blockchain to independently verify the validity of data. Although some blockchains do allow for deletion of blocks or a reset of the chain, such measures are atypical and often viewed as seriously detrimental to the protocol's credibility.

- **Transparency**: All members of a blockchain network are able to see the data on the chain, including its transaction history (unless that data is published on the blockchain in encrypted form). For people and organizations that were not previously able to share data, a blockchain provides transparency. While a blockchain network by default allows all members to see all the data on the chain, many applications now provide tools to encrypt data at the source or decrypt that data based on system permissions. This mechanism allows a network to offer the desired level of transparency while meeting privacy requirements and without sacrificing the blockchain's integrity, security, or immutability.

- **Interoperability**: One of the critical features of blockchain networks is that they can be made interoperable with one another fairly easily, so there is no need for users to onboard onto multiple blockchains in order to engage in cross-network transactions. Facilitating this communication between networks has been a priority of the blockchain industry to enable faster scaling and adoption. Importantly for financial assets like the DLPC, this trait means that one party can transact with counterparties on other blockchain networks and maintain the same level of security.

Below is an example from Skuchain, a provider of blockchain solutions for global trade, of a DLPC in the context of a full blockchain system. In Figure 1, the DLPC is minted as a non-fungible token on the blockchain to ensure its uniqueness and value. The legal agreements and any original transaction documentation can be attached to the DLPC if desired. The result is a unique digital asset for trade that is now ready for use in transactions.

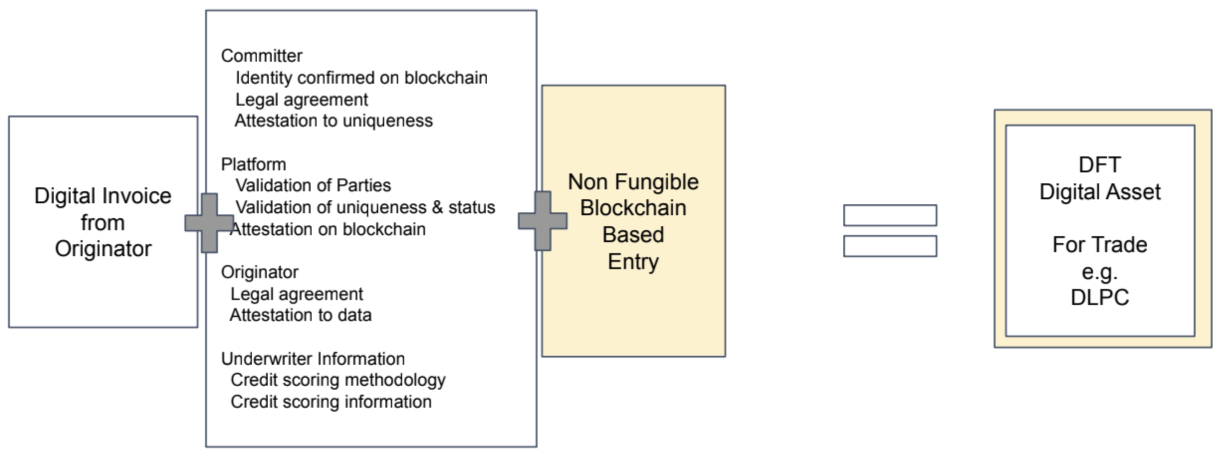

Figure 1

In Figure 2, we see that the public blockchain on which the DLPC lives (the DFT network) is part of a broader infrastructure that supports the end-to-end execution of supply chain transactions. Existing enterprise resource planning systems and private blockchains, which function much like intranets, are connected to the DFT network via APIs (application programming interfaces) so that transaction data can flow across them. The DFT network itself can be accessed through an application that allows for financial flows, security checks and smart contracts. The result is a system that integrates well with legacy systems where much of the current transaction data lives, while enabling access to a blockchain that mints and finances DLPC assets.

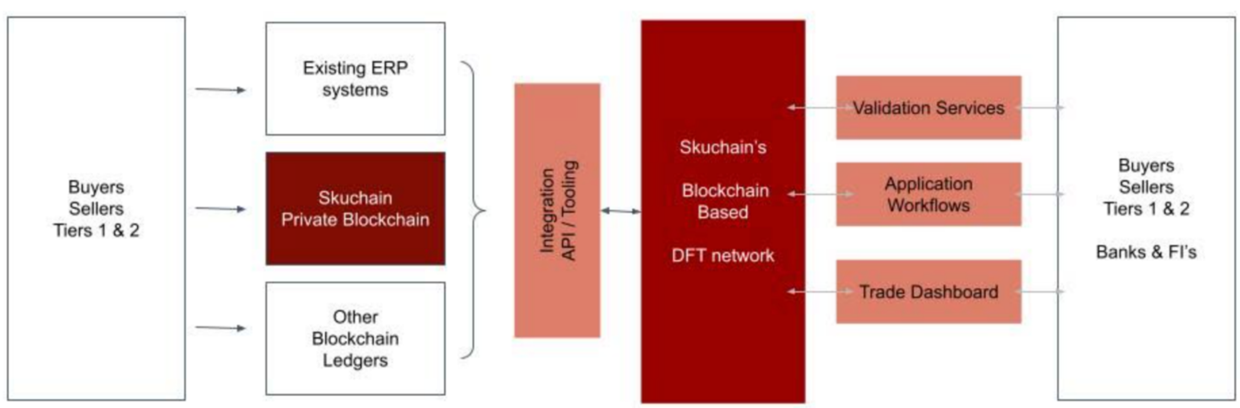

Figure 2

<u>An Example DLPC Use Case</u>

Because of the DLPC's ready transferability and compatibility with smart contracts, it is suitable for a very large number of possible use cases in financing arrangements. One example use is for so-called “deep tier” supply chain financing that allows suppliers upstream in the supply chain to receive payment more quickly and at a lower cost of capital than would otherwise be available.

In the supply chain, suppliers often receive payment substantially later than the date on which their goods are received by the buyer. In this sort of transaction, the buyer can issue a contingent DLPC to the supplier that becomes effective once the buyer confirms that it has satisfactorily completed receipt and inspection of the goods. At this point, the supplier has an unconditional promise to pay from the buyer that is paperless and instantly and securely transferable on the blockchain. The promise also can be independently authenticated by any permissioned network participant. Upon receipt, the supplier can receive immediate cash by selling the DLPC to a bank or other third party. This sort of transaction can also be conducted automatically by smart contract.

Because the DLPC greatly reduces the risk of fraud and documentary errors and is treated similarly to a negotiable note, virtually the only payment risk associated with the DLPC is the issuer (in our example, the buyer) becoming insolvent. Accordingly, if the buyer has a strong balance sheet, the supplier should be able to sell the DLPC at only a small discount, essentially leveraging the buyer’s credit for the supplier’s own supply chain financing—but at minimal cost to the buyer. In this way, the supplier can accelerate its receipt of cash on significantly better terms than would be available through a factoring arrangement or other similar financing scheme. The buyer might take advantage of this dynamic to negotiate a reduction in the purchase price of the supplier’s goods in exchange for the issuance of a DLPC. In this case, both the buyer and the supplier have a financial incentive to utilize DLPCs in their transactions. By using the DLPC, the parties are able to leverage the buyer’s strong credit to their mutual advantage while digitizing and streamlining the associated documentation.

This structure can be replicated throughout the supply chain such that upstream suppliers receive financing ultimately backed by the credit quality of the anchor buyer. A tier one supplier, for example, can issue its own DLPC to the tier two supplier, and so on. Furthermore, if desired, the tier one supplier’s DLPC can automatically transition from contingent to effective upon the effectiveness of the buyer’s DLPC. A nearly unlimited array of configurations and customizations are possible.

DLPC Compliance with MLETR

In 2017, the United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Transferable Records, or MLETR, a legal framework under which jurisdictions may deem electronic transferable records to be valid. Historically, including in the United States, no such framework existed. And while many laws have been implemented to accept electronic signatures or documents, they have often failed to address electronic transferable records.

Because the DLPC is an electronic version of a negotiable instrument, it is included within the scope of MLETR. Under MLETR, all e-negotiable instruments, including the DLPC, are to be deemed no less effective, valid or enforceable than their paper equivalents, provided that they fulfill certain requirements. If a jurisdiction adopts MLETR, this rule would govern the DLPC. To date, Bahrain, Singapore, Belize, Kiribati and Abu Dhabi have formally adopted MLETR, and the G7 indicated support in principle when it agreed to facilitate the adoption of electronic transferable records.

While MLETR provides a legal framework, including certain required properties, for valid and enforceable e-negotiable instruments, it does not specify the format for such instruments. That work is left to standards bodies and individual software platforms. Recognizing this, BAFT and its partners released the DLPC best practices with the requirements of MLETR in mind.[2]

Most importantly, under MLETR all required properties must be executed in a reliable system. The metrics for reliability are purposefully broad to accommodate many possible technology platforms, including those not based on blockchain. However, a well-designed blockchain network that implements the technical characteristics discussed above would meet the MLETR requirements of reliability.

Conclusion

The DLPC represents the careful application of blockchain technology to digitize a legal concept—the negotiable instrument—that has existed for centuries. The characteristics of blockchain networks are particularly well-suited to this exercise, allowing levels of security, verifiability, transparency, and network interoperability that, as a package, are simply unavailable through other solutions. Additionally, the DLPC allows for the digitization, streamlining and automation of manual, paper-based processes that would be required with alternative financing arrangements. Due to the DLPC's flexibility and potential application to a wide array of transaction types, businesses and banks should seriously consider how the instrument might improve their operations, accelerate cash flow, and reduce costs.

---

[2] Specifically, MLETR requires that an electronic transferable record have the properties listed below. The corresponding specification in the DLPC technical best practices is indicated in parentheses next to the applicable property below.

- An e-signature (Section 2)
- Identification of the record as an electronic transferable record (Section 4.1)
- Clear control by a person or party of the record on the system until the record is no longer valid or effective (Sections 4.10 and 4.11)
- Integrity of the record, which allows for authorized changes but no other alterations outside of normal course changes for communication, storage and display (Section 3)
- Date, timestamp and location, if applicable (Section 4.2.2)
- Records of endorsements, if any are required for that record (Section 2)
- Clear indication if the electronic transferable record is meant to replace its paper counterpart, in which case the paper counterpart ceases to be valid (Section 4.3)

Rebecca Liao was Co-Chair of the DLPC Working Group at BAFT and is Co-Founder, Advisor and former COO at Skuchain. Reid Monroe-Sheridan is an Associate Professor at Keio University Law School in Tokyo, Japan, and a Japan Advisor for Skuchain.

The opinions in this article are those of the authors and not of CodeX, Stanford Law School, or Stanford University, and CodeX, Stanford Law School and Stanford University do not endorse any of the entities mentioned.

This article is for general informational purposes only. It does not, and is not intended to, provide legal advice. Information in this article may not be up to date. Any party seeking legal advice must engage its own legal counsel.