Application of Distributed Ledger Technology to Financial Services Regulation and Compliance
International, USA (National/Federal) Related Content

A Practice Note examining how blockchain and distributed ledger technology (DLT) can facilitate regulatory compliance in banking and financial services, saving time and expense, and preventing errors. The Note details a test case for the application of DLT to regulatory compliance using the example of CFTC swap data reporting regulations.

Rising regulatory and compliance costs have led financial institutions to seek solutions using new regulatory technologies, popularly referred to as RegTech. This new field has become a key component of the efforts of financial institutions to comply with the expanding set of global financial regulations that followed the 2008 financial crisis, including:

- The Dodd-Frank Act (see Practice Note, Road Map to the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010).
- The European Market Infrastructure Regulation (EMIR) (see Practice Note, EMIR: Overview).
- Basel III (see Practice Notes, Basel III: Overview and The Final US Basel III Capital Framework).
- Global know-your-customer (KYC) and anti-money-laundering (AML) rules (see Practice Notes, USA PATRIOT ACT and Know Your Customer Requirements for Lenders and US Anti-Money Laundering and Trade Sanctions Rules for Financial Institutions).

In each of these cases, ensuring data integrity has emerged as a key concern (see Ensuring Data Integrity and Data Lineage). Financial institutions need to be able keep and maintain high-quality data in order to undertake compliance obligations to:

- Report data.
- Analyze risk.
- Maintain reliable, auditable records.

Regulators have highlighted this as a key concern, including in both the Basel Committee on Banking Supervision (BCBS) Principles for Effective Risk Data Aggregation and Risk Reporting (see Legal Update, BCBS Consults on Principles for Effective Risk Data Aggregation and Risk Reporting) and attestation requirements from the Federal Reserve Board.

These compliance goals are further complicated by large bank IT systems that are costly to maintain and require an expanding number of **bespoke** software solutions to compensate for their limitations. Over decades, banks have grown, merged, been acquired, built new service offerings, and in the process adopted fragmented infrastructure across business lines. The result is a patchwork of systems, often incompatible, spread across multiple jurisdictions.

RegTech and DLT

RegTech – short for regulatory technology – is an evolving industry designed to provide solutions to particularly complex or difficult processes that financial institutions must undertake to comply with their post-crisis regulatory obligations.

More recently, **blockchain** or **distributed ledger technology** (DLT) has emerged as a key component of next-generation RegTech and financial infrastructure. While most attention has been focused on the potential for DLT to transform the basic infrastructure underlying many of the world's financial markets, these changes will ultimately impact the way those markets are regulated and the way banking regulation is complied with.

By offering a new architecture for financial services, DLT can ease compliance burdens by reducing some of the complexity of the regulatory-compliance procedures that financial institutions undertake. Not only can regulatory compliance be made more efficient, but the technology presents new opportunities for regulators to design better, smarter regulations that can promote efficient, safer markets while reducing costs to regulated entities.

This Note discusses how DLT offers both financial institutions and regulators new tools for facilitating regulatory oversight. In particular, it:

- Provides an overview of distributed ledgers in financial services.
- Explains the application of DLT to regulatory procedures.
- Highlights opportunities for innovation in RegTech.
- Describes a test case for using DLT.

Overview of Distributed Ledgers in Financial Services

Distributed ledgers allow multiple parties to jointly view and edit one shared, consistent record of information. Rather than maintaining separate records of important information – for example, a balance of cryptocurrency in an account or the state of an agreement between parties – a distributed ledger provides one single record of this information that is jointly held and managed by multiple parties. Each party holds a copy of the record, is able to view it, and may be able to update it, but each copy is synchronized with all others through what is known as a "consensus algorithm."

A distributed ledger is maintained by a group of computers called nodes. These nodes form the network that supports the distributed ledger: They each update the ledger to reflect any transactional developments and enforce its basic rules, and each keeps its own copy of the ledger. In this way, the ledger is "distributed" or "decentralized," meaning that no central party is responsible for it, but rather a group of participants that jointly manage it. Some distributed ledgers have many thousands of nodes spread across the world, while others might only allow a handful to participate in a closed network.

An Example: DLT Smart Futures Contracts

DLT can be used to create a smart contract, which is a contract that is self-executing on the blockchain without the need for further action by the parties. For example, two parties intend to enter into a simple financial agreement, such as a **futures contract** based on the price of gold. The parties would record the terms of the gold futures contract on the distributed ledger itself. There would not be separate copies of the gold futures contract, but rather one (digital) contract to which both parties have access. As the contract moves through its life cycle, the ledger keeps a history of every change and update, creating an authoritative audit trail of the entire transaction.

Many **smart legal contracts** of this kind need to rely on a trusted source of outside information known as an oracle. The oracle can be a financial services provider or another reliable, mutually agreed third party that provides information, such as an interest rate, commodity price, or index price. In the gold futures contract example, an oracle provides the price of gold, which is necessary for the gold futures contract to settle.

The contract would be at least partly articulated in smart contract code, meaning that when certain triggers are met – for instance, by checking the price of gold on an agreed-on date – the contract can settle automatically, resolving the outcome of the contract.

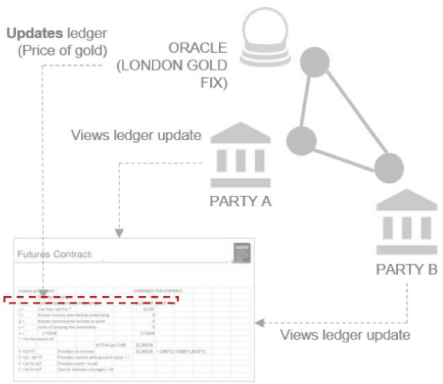

Diagram: An oracle is used to obtain the price of gold, which is necessary to settle the gold futures contract.

Applying DLT to Regulatory Procedures

Broadly, regulatory compliance involves the following five general procedures:

- Recording and reconciliation. This is the foundational requirement for regulatory compliance (see Recording Information).
- Aggregating data. This is required where, for practical or legal reasons, data is stored on multiple systems or in multiple locations (see Aggregating Data).
- Ensuring data integrity and data lineage. While a trade moves through multiple systems during the trade lifecycle, data can be altered and deleted (see Ensuring Data Integrity and Data Lineage).
- Performing operations on data. Data used in regulatory reporting must often be processed or analyzed before being submitted to a regulator. For example, it may be necessary to apply internal financial models to determine compliance with capital-adequacy requirements or, more superficially, convert data into a required format. (For more information, see Performing Operations on Data.)
- Sharing information with other entities. Regulatory reporting obligations require that firms be able to share information securely with regulators and occasionally with other entities (see Sharing Information).

Considering how each of the above procedures would be accomplished using DLT provides a clearer understanding of the technology's potential to address regulatory challenges.

Recording Information

Complying with financial regulations requires recording and securely storing data. Firms often rely on automated systems to capture transaction data from trading platforms and store it securely, where it can later be processed into the forms necessary for financial reporting. In other cases, firms may rely on manual procedures to record information about financial events.

Many firms are legally required to retain records of certain information about their clients and their clients' business activities for a specific period of time. This includes, for example, the Financial Crimes Enforcement Network (FinCEN) requirements to keep and maintain account-opening data or the obligation of firms to record and regularly publish financial information.

The procedures used to capture, record, and store this data can be simplified using DLT. When a distributed ledger is used to perform a basic financial function, such as tracking account balances or the state of an agreement between parties, this data is stored in a single authoritative source: the distributed ledger. Instead of creating a record of financial information – for instance, by capturing data from a trading platform and storing it in a separate database – a party may simply refer to the transaction itself, as recorded on the distributed ledger.

The current challenges in matching counterparty trade reports illustrate how DLT could help parties resolve recordkeeping compliance issues. Under EMIR, every derivatives contract must be assigned a Unique Transaction Identifier (UTI). Under European law, both parties to the trade must report it to a data repository, and the UTI is used to match those reports to one another. However, this process is prone to errors. UTIs may be generated incorrectly or not properly shared between parties. In 2014, the **Depository Trust and Clearing Corporation** (DTCC) reported that it was able to match only 40% of the trade reports it received. Similar issues exist with **legal entity identifiers** (LEIs).

Use of a distributed ledger would resolve this counterparty-matching issue entirely. Instead of each party holding separate records of a trade, the parties share one record. This eliminates any confusion on contract terms and conditions, and ensures each party records the same information in its internal systems. A UTI, an LEI, or any other information included within the record of that trade would remain shared and accessible between each party that has access to the digital record of that transaction. It would therefore be impossible to "mismatch" reports, because there are no reports to match. There is only a single authoritative record, recorded on the distributed ledger.

More fundamentally, use of a distributed ledger would likely eliminate for UTIs, since they were introduced primarily as a method for trade reports to be matched, which is unnecessary on a distributed ledger. If it were necessary to identify a particular transaction or record, the unique hash of the data could be used, rather than a UTI.

Aggregating Data

Regulatory procedures typically require aggregation of data from multiple sources. Many financial institutions operate multiple, sometimes incompatible, legacy IT systems that require complex aggregation procedures to draw together the necessary data into a single record or regulatory

report. In other cases, the information required for certain regulatory reports may come from different business lines, which may operate in different jurisdictions. This further complicates reporting.

This is not simply a technical problem that can be solved using a distributed ledger. There are practical and legal reasons that data will always be stored across multiple sources. For instance, certain recovery and resolution rules require systemically important banking functions to operate independently of each other, sometimes in distinct legal entities. Data localization and privacy laws may require that certain information remain within national borders, necessitating multiple data sources for certain regulatory reports for a multinational financial institution.

Aggregation is still necessary, even with the application of DLT. However, the process of combining data sources from multiple DLT platforms would simply involve collecting a series of links that point toward a set of records on a distributed ledger. Again, rather than creating a separate repository of data that has been aggregated from other sources, there would instead be a comprehensive live view that reflects the information stored in the authoritative ledger. This could facilitate compliance with Basel III and similar regulations that require banks to understand their liquidity position across multiple products, in multiple jurisdictions, at a single point in time.

Ensuring Data Integrity and Data Lineage

Firms employ procedures designed to ensure data integrity throughout all of the procedures described in this section. For instance:

- Reconciliation between different entities to ensure that their records continue to match over time.
- Creation of metadata that provides an auditable trail for particular records.

Many of the errors in these procedures would be avoided simply through the use of a distributed ledger. For example, if firms do not need to make multiple copies of a data set for distribution among many parties, there are fewer opportunities to introduce errors. Reliance on a single authoritative ledger would reduce errors and the need for separate reconciliation, verification, and auditing using multiple systems.

Compliance procedures require that financial institutions maintain authenticating metadata that can be used to attest to the origin of certain information and track its history from creation to reporting. Distributed ledgers achieve this by maintaining a complete record of every update or change (state change) in its history. A distributed ledger also automatically produces an auditable trail and full history. Anyone provided with the correct permissions, such as a regulator, would be able to view the history and status of any particular financial agreement or transaction.

For example, on Ethereum, a regulator could view the history of a given contract by looking "back" to each block since the creation of the record for that contract. On a permissioned ledger such as Corda, a regulator would be given access to what is referred to as a "state-object" that represents a financial relationship (technically, the data would be "pushed" to the applicable regulator). On certain other ledgers, the applicable regulators may be given a digital key (which could be automated) that allows them able to view a transaction's history on the ledger. This process is described in greater detail under A Test Case: Reporting of OTC Interest Rate Swap Transaction Data Using DLT.

Generally, parties would prefer that their data-integrity control procedures are applied prior to performing operations on data or sharing data (including regulatory reporting), after the aggregation stage.

Performing Operations on Data

Regulators often require that firms process or analyze data, rather than simply record or report it. For example, firms must apply internal models to determine whether they meet certain capital-adequacy or other risk requirements (for example, under Basel rules) based on their own internal data. Firms also must prepare data into a report that meets specific regulatory standards or that conforms to inconsistent legal definitions of key financial terms in different jurisdictions.

DLT does not remove the need for financial institutions to analyze data. Risk reporting will always require analysis of large data sets to determine the risk profile of a given financial institution and whether it meets a certain standard. However, if distributed ledgers provide higher quality data with fewer errors, this could have implications for regulatory procedures involving analysis.

For instance, a bank can fail Comprehensive Capital Analysis and Review (CCAR) due to data quality issues and the inability to trace that data to its source, even where the bank has sufficient liquidity to manage a stress scenario. Raising data quality across the industry would allow regulators to focus on conducting meaningful analysis drawn from the distributed ledger rather than spending time processing the data, which in many cases involves understanding the individual systems of record at each financial institution. Higher confidence in the data underlying these models could be a basis for reducing or at least refining capital requirements without necessarily increasing risk.

Sharing Information

Reporting obligations require that firms be able to share information securely with regulators. Several blockchains allow regulators access to information on a ledger. For example, Corda has a regulatory node that allows banks to send data to regulators in a read-only mode. This allows regulators to receive information in almost "real time." Not all transactions are required to be reported in real time, so different parameters can be set depending on reporting frequency. Ultimately, the bank is still in control of its transaction information and can submit only relevant information to a regulator.

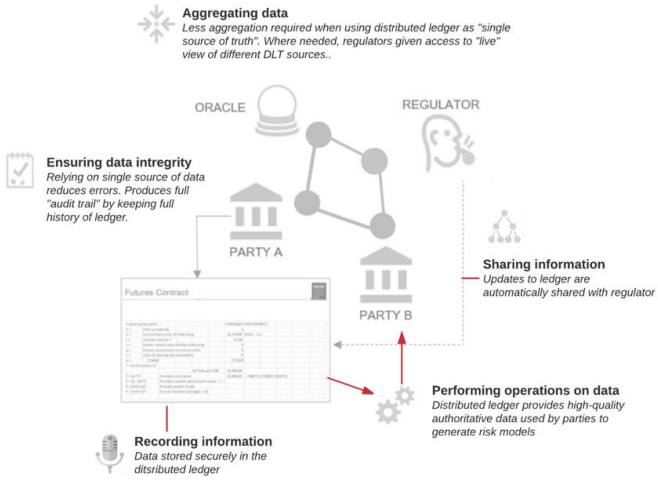

Diagram: Distributed ledger technology applied to basic regulatory procedures.

Opportunities for Innovation in RegTech

While distributed ledgers can be used to facilitate and improve on existing regulatory procedures, the new model for financial infrastructure offered by DLT may provide new tools to promote more efficient and reliable compliance.

With reporting and reconciliation much easier on a DLT platform, a regulator may require data to be submitted in near real time, as opposed to, for example, every 90 days. This would help detect warning triggers of a downturn much earlier. The ease of reporting would also allow regulators to request additional reporting fields for a transaction. Currently, adding new fields in a bank system is a large cost burden.

Further, with DLT, the marginal cost of reporting additional on-ledger information to a regulator is also low. This not only reduces costs for financial institutions, but it might also enable regulators to obtain more reporting than currently, while still lowering overall costs to the industry.

DLT could also allow firms to adapt more easily to changing regulatory requirements. Reacting to a new regulation that requires additional reporting would in many cases be as simple as "un-hiding" data that was previously hidden from the regulator, and continuing to provide access to that ledger for that regulator.

Further, DLT may also enable new methods to enforce regulatory compliance. The examples considered above have focused on how firms record, manage, share, and verify data. However, other regulations require firms to follow certain procedures. KYC and AML regulations are one example: When engaging in certain activities, such as opening bank accounts or transferring funds, firms must verify the identity of their customer or counterparty according to a legal standard (see Practice Note, USA PATRIOT ACT and Know Your Customer Requirements for Lenders: General Application of the Customer Identification Program).

DLT would make it possible to enforce regulations more directly. Rules can be built into the platform itself or into a specific application on top of the platform so that certain transactions would only complete when specific conditions are met (such as the furnishing and verification of required information).

For example, a requirement that a counterparty provide sufficient documentation, such as a driver's license and proof of address to confirm its identity, can be embedded into the logic of a transaction to comply with KYC standards. The client would only complete onboarding once the bank received all KYC documentation and an oracle or other trusted third party attested that the information provided is correct.

With this type of "compliance by design," the mechanism used to carry out basic banking functions would be constructed to follow a certain rule, and the code that executes that rule would be visible to regulators. Because regulators would be able to see and verify for themselves that a given contract contains code that enforces the rule, regulators could have greater confidence in this process than the current one, which, as has been documented by regulators, has proven prone to inconstancy, error, and inaccuracy (see Legal Update, CFTC Issues Advisory and Request for Comment on Swap Data Reporting).

Privacy in DLT: Permissioned Ledgers

One fundamental challenge for DLT is preserving the privacy and confidentiality of participants and their data. Users of a distributed ledger – in particular, financial institutions – may not want to share the details of every financial relationship with every participant in a distributed ledger, which may include competitors. Further, in many cases legal requirements may prevent financial institutions from sharing data or storing it outside of certain jurisdictions. Data privacy has therefore emerged as a critical design issue for DLT use in regulated industries and regulatory procedures.

Permissioned ledgers can address these concerns by limiting access to certain data for particular entities. In this way, permissioned ledgers follow the model of existing financial infrastructure and are able to protect privacy and confidentiality in a manner that is familiar to financial institutions.

Public blockchains like bitcoin or Ethereum do not limit access to their ledgers. They are:

- Open, in that anyone can participate in the network by "running a node" on the ledger.
- Transparent, in that the details of all transactions are replicated to all nodes and visible on the ledger to all participants.

The European General Data Protection Regulation (GDPR) ((EU) 2016/679), which became effective in May 2018, illustrates the privacy challenges for DLT. The GDPR restricts how information about European Union (EU) citizens may be used. Many of the obligations under the GDPR would be difficult to comply with for any entity using a public blockchain to store information pertaining to EU citizens. For example, the "right to be forgotten" under the GDPR allows an individual to demand the erasure of information under certain conditions, which would be impossible in many cases with a public blockchain.

The GDPR also imposes requirements on data that is transferred outside of the EU. However, compliance with the GDPR data transfer requirements would be impossible for an entity using a public blockchain, because the recipients (nodes) that hold the data outside of the EU, as well as their location, would be unknown. As a result of these and other related issues, use of public blockchains could create violations of the GDPR.

Because of these issues, privacy- and confidentiality-protection technology for blockchains is an active area of research and development in DLT. Certain technologies have been developed that can protect the identity of a participant by hiding the public key that provides access to a node (and therefore data) for a transaction. These technologies include:

- Ring signatures.
- Stealth addresses.
- Pedersen commitments.
- The enigma protocol.

Some of these technologies could hide transaction or computation data. Implementation of these technologies in blockchains may be recent, but the underlying cryptography is mature and well understood. More recent cryptographic techniques, such as zeroknowledge proofs (which were implemented in the fully-anonymous cryptocurrency Zcash), allow for even greater privacy and confidentiality guarantees. However, in some cases even mature cryptographic techniques may not be a sufficient solution. While some cryptographic methods may be essentially impossible to break with today's technology, that may not be true in the future.

Privacy- and confidentiality-protecting techniques, such as anonymizing data on a distributed ledger, is an active area of research in DLT. Some combination of these techniques might offer sufficient protection to enable, for example, data stored on a blockchain to no longer be considered "identifiable" within the meaning of regulations such as the GDPR.

For now, the comparatively low-tech solution of limiting read-access may be the most practical method for financial institutions to meet their legal data treatment obligations.

A Test Case: Reporting of OTC Interest Rate Swap Transaction Data Using DLT

With a DLT permissioned ledger, compliance with applicable **Commodity Futures Trading Commission** (CFTC) swap data reporting rules enacted under Title VII of the Dodd-Frank Act for an **over-the-counter** (OTC) **interest rate swap** (IRS) can be achieved with greater efficiency.

An IRS is a contract under which two parties exchange streams of interest payments: One party makes interest payments based on a fixed rate, while the other party makes payments based on a floating rate such as **LIBOR** or another benchmark (see Practice Note, Finance Fundamentals: Deconstructing Derivatives: Basic (Plain Vanilla) Interest Rate Swap). The parties make payments to one another on regular payment dates (for example, quarterly or monthly) during the term of the agreement.

Post-financial crisis regulatory reforms such as Title VII of the Dodd-Frank Act introduced new data reporting obligations for OTC derivatives (see Practice Note, Summary of the Dodd-Frank Act: Swaps and Derivatives: Dodd-Frank Swap Data Reporting and Recordkeeping Requirements). Before the enactment of these regulations, OTC derivatives were typically entered into **bilaterally**, between individual firms, and were not required to be reported to a regulator.

For OTC IRS, which are governed by the CFTC, there are two primary components to these regulations.

- Real-time public reporting of swap transaction data under Part 43 of the CFTC regulations. This data must be reported to a **swap data repository** (SDR) shortly after execution of the swap (see Practice Note, US Derivatives Regulation: CFTC Swap Data Reporting and Recordkeeping Rules: Part 43 CFTC Real-Time Public Swap Data Reporting Rules).
- Regulatory "SDR" reporting of swap transaction data under Part 45 of the CFTC regulations. This data is reported to an SDR and then passed along by the SDR to the CFTC (see Practice Note, US Derivatives Regulation: CFTC Swap Data Reporting and Recordkeeping Rules: Part 45 (SDR) Data Reporting Rules).

The swap data reporting requirements under these sections could be satisfied for an IRS transaction by executing on a permissioned ledger such as Corda.

Note that this example focuses on swap data reporting requirements under US law, though many of the procedures described below could be adapted to similar requirements in other jurisdictions.

Pre-Trade Transparency and Execution for Bilateral OTC IRS Using DLT

This example assumes that the parties already have an **ISDA Master Agreement** (ISDA Master) and **Credit Support Annex** (CSA) in place, setting out the basic terms and collateral arrangements between the parties for all IRS between them.

In this example, Party A and Party B seek to enter into an IRS. Both parties have access to the same ledger, and each party maintains a node (or more likely, several nodes) on that ledger that allows the parties to form and enter into agreements.

The parties would:

- Use smart contract template agreements to enter into their IRS (crypto IRS).
- Negotiate through a user interface connected to a permissioned ledger.

The offer and final acceptance of terms would be managed through a DLT "flow framework," which is a protocol for communication between parties. As part of this flow framework, a transaction is formed on the ledger, capturing the terms of the IRS agreement between the parties. The transaction is signed and validated by each party's node. A notary is designated that is responsible for obtaining consensus over future updates.

In this case, there is also a regulator node on the network. As specified in the transaction's flow framework, the SDR or regulatory node is included in the set of nodes that are able to see details of the IRS between Party A and Party B. The initial transaction is broadcast to the regulator node, as well as confirmation from a notary that the transaction has been approved. The flow framework also specifies that any subsequent updates to the state of the IRS will also be available to the regulator node. For the purposes of this analysis, we assume that the regulator node is operated by an SDR.

Once the transaction has been validated and signed by each party's node and the flow is completed, a state-object is created to represent the IRS, which includes references to the ISDA Master and CSA. At this point, the parties have entered into the IRS, and reporting obligations are triggered.

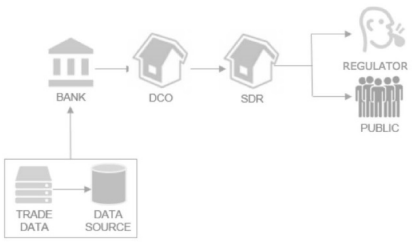

Diagram: A generic overview of the process of reporting transaction data on centrally cleared OTC trades.

Post-Trade Transparency for Bilateral OTC IRS Using DLT

Part 43 Real-Time Swap Data Reporting

Part 43 of the CFTC's regulations (17 C.F.R. §§ 43.1 to 43.7) requires certain information to be reported in real-time to an SDR (see US Derivatives Regulation: CFTC Swap Data Reporting Required Data Fields Checklist: Required Data Fields Under Final CFTC Real-Time Swap Data Reporting Rules (17 C.F.R. Part 43)). This data must include:

- Time and date of execution.
- An indication of whether the swap is collateralized.
- Start and end dates.
- Settlement currency.
- Asset class.
- Other details about the transaction.

The regulatory node, operated by an SDR, can receive this data directly from a bank. The flow framework designed for the blockchain IRS specifies that when the IRS is created, the necessary data is "pushed" to the SDR node. Both the parties and the regulator node will have received the notarized transaction as a matter of course, and each will have used it to update its copy of the shared state-object. Rather than receiving a separate report attesting to the facts of the transaction between Party A and Party B, the SDR has an authoritative copy of the contract itself. Any changes made by either party would be resubmitted to the SDR.

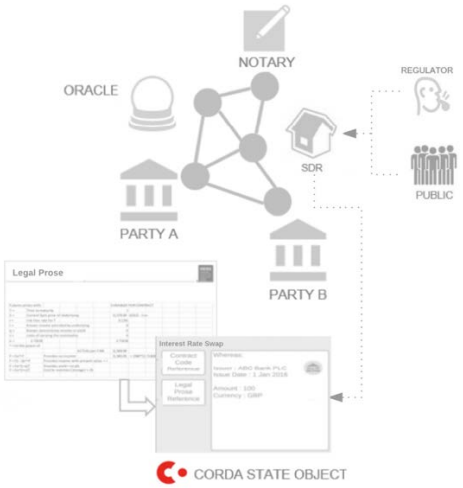

Diagram: Regulator node operated by an SDR has access to the state-object representing the transaction, fulfilling data reporting obligations.

However, certain information required under Part 43 may not necessarily be included in the crypto IRS. For example, many IRS are subject to a mandatory clearing requirement under Title VII of the Dodd-Frank Act, meaning that they must be cleared by a **derivatives clearing organization** (DCO) (see Practice Note, US Derivatives Regulation: Swap Clearing and Exchange Trading: Swap Clearing Under Title VII). However, there are certain exceptions to that requirement, such as the commercial end-user exception (see Practice Note, US Derivatives Regulation: The Commercial End-User Exception to the Mandatory Swap Clearing Requirement).

Part 43 requires that, for any trade not centrally cleared, the parties must indicate in the report for that trade the legal exception or exemption from the clearing requirement that the parties are relying on. More generally, for certain reporting obligations, there may be data that must be reported that would not ordinarily be included in the legal contract or confirmation letter for the relevant transaction and thus not included in the crypto IRS.

However, the solution is simple: In order to ensure that the relied-on exception or exemption is reported to the SDR, this information would be included in the contract itself, or as an attachment. This means that the SDR receives this information along with the terms of the contract.

To complete the Part 43 reporting process, the SDR would extract the necessary information from the state-object, anonymize it, and report it publicly through the same process used currently.

One component of the real-time reporting obligations under Part 43 offers an opportunity for automation and, perhaps, more finely tuned regulation: Part 43 includes a rule under which certain "block trades" of sufficiently large value are granted a time delay for when they are reported publicly. The rationale for this rule is that real-time reporting of these large trades can reduce market liquidity and disproportionately impact the market (see Practice Note, US Derivatives Regulation: CFTC Swap Data Reporting and Recordkeeping Rules: CFTC Block Trade Rules).

For example, Corporation A raises capital by issuing a fixed-rate bond. Corporation A may choose to hedge its interest rate risk on the bond by entering into an IRS with Bank B. If this large IRS is publicly reported, it could signal to the market that someone (Bank B) will be seeking a way to hedge its risk from that transaction. This can lead other entities to adjust pricing in anticipation of a trade, increasing costs to Bank B, which therefore may decline to enter into the transaction with Corporation A, or to raise its own price to Corporation A.

A DLT reporting structure like the one described above offers opportunities to automate this process. The regulator node would automatically check the value of any given IRS, and according to pre-defined smart-contract code, would trigger a reporting delay if the value exceeds the current minimum block size that would trigger the delay. This, in turn, could enable regulators to fine-tune reporting delays according to transaction size, as opposed to a blanket "minimum" that triggers a standard delay.

Assuming there is a function that expresses the relationship between trade size, reporting delay, and impact on market liquidity, then that function could be built into the transaction framework for each crypto IRS, triggering the appropriate reporting delay automatically for trades of every size.

Part 45 Swap Data Reporting and Recordkeeping Requirements

Under Part 45 of the CTFC's regulations (17 C.F.R. §§ 45.1 to 45.14), parties must report both creation data and continuation data for a swap:

- **Creation data** includes:
  - the Primary Economic Terms (PET) of a swap, which, for an IRS, includes information such as asset class, execution venue of the swap, start and end dates, and price (see US Derivatives Regulation: CFTC Swap Data Reporting Required Data Fields Checklist: Primary Economic Terms (PET) to Be Reported Under Final Swap Data Reporting (SDR) Rules (17 C.F.R. Part 45)); and
  - **confirmation** data, which includes the commercial or economic terms of a swap, such as strike price, **notional amount**, and contract type agreed by the parties, as well as certain identifying information for cleared swaps.

(See Practice Note, US Derivatives Regulation: Practical Guide to Over-the-Counter (OTC) Swap Data Reporting.)

As under Part 43, this information must be reported to an SDR as soon as technologically possible. Under the example above, this information is automatically pushed to an SDR by virtue of the SDR node's inclusion in the flow framework for this transaction.

- **Continuation data** is data that is reported throughout the life of the swap in order to ensure that the information held by the SDR remains current and accurate. Continuation data has two components:
  - **life-cycle data**, which includes any event that alters the PET of the swap – for example, if the terms of the swap are amended by the parties. Because the SDR node is part of the flow framework for this transaction, it (and by extension the applicable regulator) will automatically be aware of any alteration to the PET; and
  - **valuation data**, which is "all of the data elements necessary to fully describe the daily mark of the transaction" that must generally be reported to the SDR daily.

Valuation Data Reporting Under CFTC Rules

Reporting daily valuation data is more complex than reporting life-cycle data. Reporting life-cycle changes to the IRS is simple because the SDR already has access to the state-object, since the transaction's flow framework says that any update is sent to the regulator node. However, valuation data requires a separate process that can incorporate outside information, such as drawing market data from an oracle. (Additionally, both parties to the IRS may not need to receive daily valuation data. Only the SDR/regulator node may need to receive it.)

One way to achieve this would be to create a separate "valuation state-object." This state-object would refer to the IRS state-object and be incorporated into the flow framework used to create and manage it, but would be a separate state-object. Like the IRS state-object itself, the valuation state-object would be shared with the SDR/regulator node. By using a separate state-object, the problem of having to "update" the IRS state-object every day with new valuation data is avoided.

Each day, the reporting party tasked with submitting valuation data would form a new transaction on the ledger (which could be automated). This transaction would take the existing valuation state-object as an input, and output a new valuation state-object. The transaction would essentially update the valuation seen by the regulator node each day with the information necessary to disclose the daily mark of the swap. The state-object would also include the methodology and assumptions used to prepare the mark, as required under CFTC regulations.

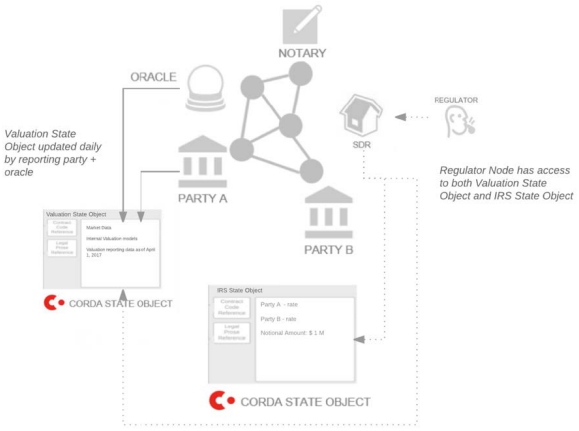

Diagram: Regulator node operated by the SDR has full view of valuation state-object, which is updated daily to satisfy CFTC Part 45 valuation-data reporting obligations.

Additional Considerations

Centrally Cleared Swaps

Under CFTC regulations, certain types of swaps must be centrally cleared by a DCO. With clearing, the DCO steps into the middle of the trade, "guaranteeing" each party's performance under the transaction, and essentially creates two trades for each cleared derivative (see Practice Note, Mechanics of Derivatives Clearing: Two Models: Clearing Member as Agent or Principal).

For centrally cleared swaps, the DLT data reporting process outlined above would be slightly different. The terms of the IRS negotiated between the parties would be the same, but the final agreement represented by the state-object would be broken into two transactions, each facing a third party, the DCO. Like the other parties to the transaction, the DCO would operate a node on the platform for this purpose.

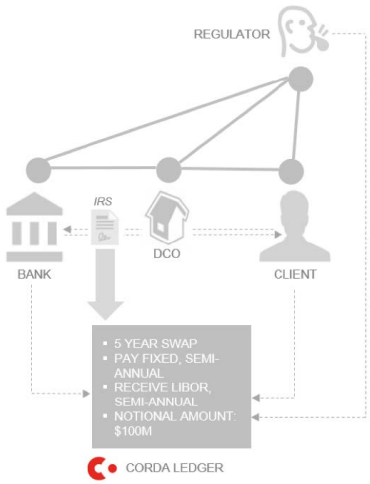

Diagram: A centrally cleared swap, where a DCO sits "between" two parties to an IRS.

Reporting Party Responsibility

Parts 43 and 45 set out rules determining which party is responsible for reporting specific information. Under Part 45, the DCO is responsible for reporting the data for any swap that is subject to mandatory clearing (see Practice Notes, US Derivatives Regulation: Practical Guide to Over-the-Counter (OTC) Swap Data Reporting: Which Is the Reporting Party? and US Derivatives Regulation: CFTC Swap Data Reporting and Recordkeeping Rules: Cleared Swap Data Reporting Under Part 45: The Cleared Swap Rule).Most IRS in the US must be cleared, so in practice, the parties to any given IRS will likely not be responsible for reporting, as the DCO will be the reporting party.

For swaps that are not centrally cleared, one of the counterparties to the IRS is responsible for meeting the reporting obligations. In practice, if a cleared IRS were executed using a permissioned ledger, the data reporting process described in this Note would be unchanged.

Updates to the state-object (creation data and life-cycle data) may be seen by all parties included in the flow framework and, from the perspective of the reporting party, happens automatically without requiring any special effort on its part (beyond agreeing to the update itself). In practice, it is the defined flow framework between the parties that ensures information is available to the regulator node. Nonetheless, the reporting party would be held responsible if the reporting process somehow fails.

The exception to this is valuation data, as described above. Here, the reporting party (in the case of non-cleared swaps) must carry out an additional process (though it may be automated) by signing transactions to update the IRS valuation state-object described above (see Valuation Data Reporting Under CFTC Rules).

Under Part 43, if a swap is executed on a registered **swap execution facility** (SEF) or **designated contract market** (DCM), then the parties to that swap have met their reporting obligations under CFTC rules. If not, the swap is considered an "off-facility swap," in which case reporting obligations are determined by the rules described in Part 43.3(a)(3) (17 C.F.R. § 43.3(a)(3)), unless otherwise agreed to by the parties (see Practice Note, US Derivatives Regulation: Practical Guide to Over-the-Counter (OTC) Swap Data Reporting: Box, Which Is the Reporting Party?).

If we assume that a trade executed on the DLT platform is an off-facility swap, then one or the other of the counterparties will be responsible for fulfilling the real-time public reporting obligations under Part 43. As described above, transaction data reporting is automated with use of the DLT platform, as information about each swap is shared with a regulator node under the flow framework, so the reporting party's data reporting obligations for that swap are satisfied.

Conclusion

Distributed ledger is a suitable technology for achieving many of the basic procedures required for regulatory compliance. Allowing multiple parties to access a shared authoritative record offers an elegant simplification of many regulatory functions. Removing the need to send copies of information may result in fewer errors, improving the quality of data:

- Used by financial institutions to model risk.
- Used by regulators to assess risk.

The built-in features of distributed ledgers, such as requiring transaction validation at each step, and recording a full audit trail complete with cryptographic signatures, improve data integrity throughout the process of negotiation, execution, and post-trade reporting. Applying this process to transaction reporting of OTC interest rate swaps, it appears likely distributed ledger could offer advantages over current data capture and regulatory reporting systems.

Most information that must be reported under CFTC regulations can be easily shared with a regulator. Because the parties sharing an authoritative record of the IRS itself, most data (for instance, the PET of the swap) will be reported automatically simply by giving a regulator node access to the state-object that represents the IRS transaction through the flow framework (see Pre-Trade Transparency and Execution for Bilateral OTC IRS Using DLT).

In other cases, parties may need to design additional procedures to meet their reporting obligations. Information required by a regulator might not, in the normal course, be included in the text of a contract. For instance, under Part 45 a party must report whether it is relying on a particular exemption or exception to the mandatory swap clearing requirement. To be reported, this information must be included in the state-object representing a financial agreement.

Some rules could be improved by being embedded directly into the platform as smart-contract code. For instance, the reporting delays for block trades of a certain value could be triggered automatically when reported to an SDR (see Post-Trade Transparency for Bilateral OTC IRS Using DLT).

The use of distributed ledgers could, in theory, reduce the need to rely on entities like SDRs that serve as middlemen in the regulatory reporting process. Advanced privacy-preserving techniques (see Privacy in DLT: Permissioned Ledgers) could be used to anonymize data before it is released to the public, rather than relying on the SDR to carry out this function. Regulators may ultimately no longer need to rely on SDRs to serve as a central store of transaction data if all transaction data is stored on distributed ledgers to which they have access.

**Based on a research paper written by Joshua Stark for R3.*

PRODUCTS

PLC US Finance, PLC US Financial Services, PLC US Law Department