CFTC Technology Advisory Committee

October 3, 2019

Distributed Ledger Technology Sub-Committee

Presenters:

Brad Levy
Yesha Yadav
Shawnna Hoffman

Agenda

- DLT Beyond Crypto
- DLT and Data Privacy
- Market Applications
- Ongoing Questions for Policymakers

DLT Beyond Crypto

- In addition to virtual currencies, traditional finance is becoming active in adopting DLT:
  - Applications are proliferating
  - Interplay between finance and crypto is becoming clearer and more concrete.

- The parts vs the whole chain
  - Storage, movement and automation related but discreet areas
  - Functional areas from execution to safe keeping through to servicing
  - All asset classes in play globally

DLT Subcommittee Discussions (I)

Subcommittee has highlighted the promise and drawbacks of DLT

Can be useful in collateral management, trade reporting, smart contracts and payments

Can gain utility by harnessing the power of the cloud and artificial intelligence

Represents a long-term project that remains in its early cycle of development

DLT Subcommittee Discussions (II)

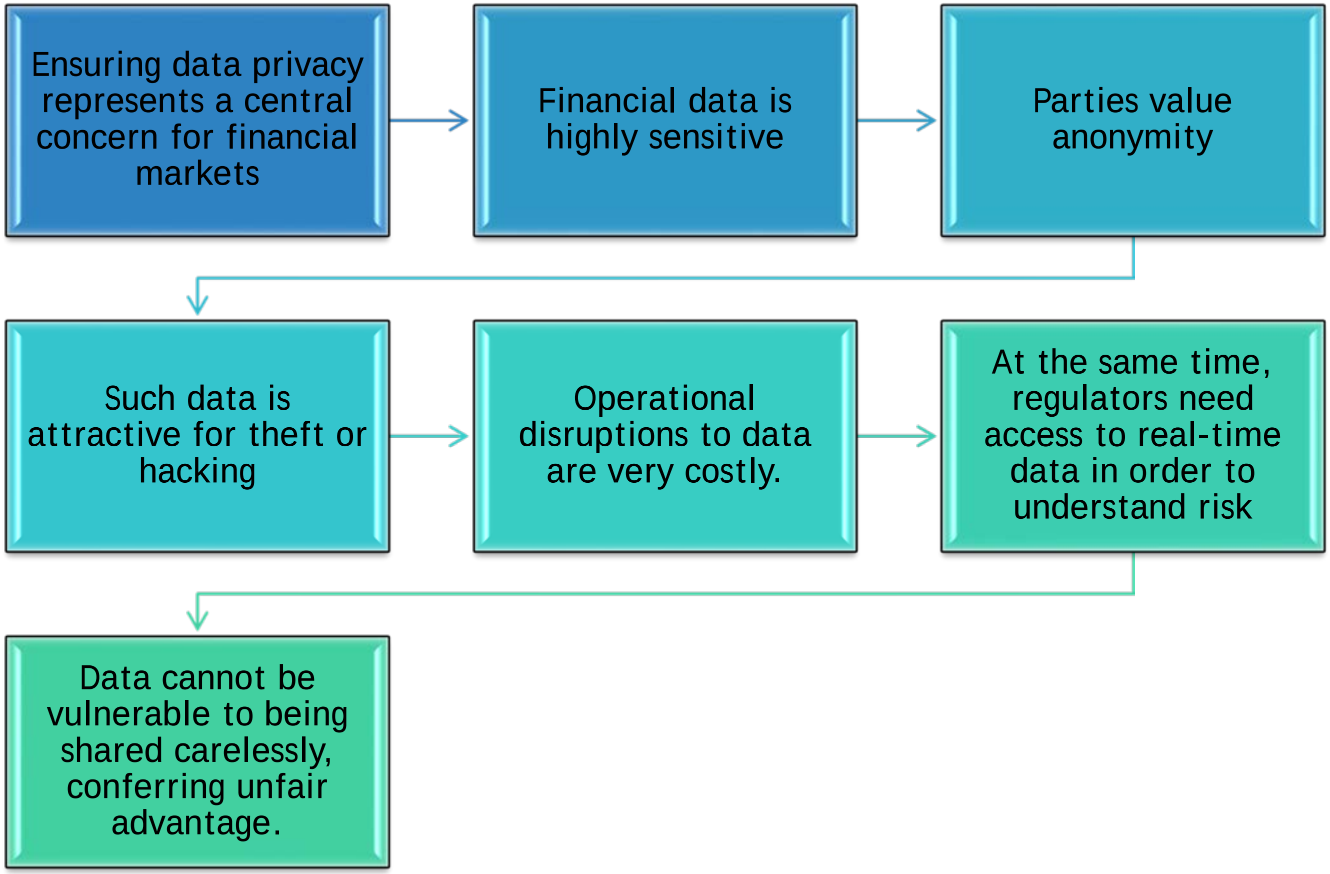
Important to consider the wider set of technologies and architectures that are rapidly evolving

From the edge to the cloud, there is a push/pull of centralized and decentralized technologies

Advancements in processing power and networking matter

Balance between data protection, automation and efficiency will drive outcomes

The Importance of Privacy



Ensuring data privacy represents a central concern for financial markets

Financial data is highly sensitive

Parties value anonymity

Such data is attractive for theft or hacking

Operational disruptions to data are very costly.

At the same time, regulators need access to real-time data in order to understand risk

Data cannot be vulnerable to being shared carelessly, conferring unfair advantage.

Privacy, Confidentiality and DLT

Privacy and confidentiality for markets can be enabled by how DLT networks are structured:

A permissioned blockchain can be created to restrict information transfer and participation between a select group of users.

For example, a permissioned network may restrict access to a small group of dealers.

It can maintain the confidentiality of trades.

DLT networks can be developed to provide users with ways to safeguard their anonymity and ensure data integrity and confidentiality.

Defining Data Privacy and Confidentiality

- A key challenge to the objective of ensuring data privacy in DLT lies in its definition
- Encryption standards constitute an essential mechanism by which DLT can secure data
- In interconnected financial markets, encryption standards must also enable interoperability
- International markets mean that the privacy offered by encryption meets with international rulemaking and standards

Encryption, Digital Identities and Securing Trading Data (I)

Encrypting user identity and trading data is critical to realizing the advantages of DLT.

In decentralized platforms, users can create anonymity and privacy through "asymmetric encryption."

Such an encryption system is based on users holding a public key as well as a private key.

A public key and private key are unique to users and are mathematically linked.

Information "signed" by user a's private key is unlocked by reference to her public key.

Encryption, Digital Identities and Securing Trading Data (II)

DLT is known for its ability to created an encrypted and immutable digital record of transactions.

- Hashing algorithms (e.g. SHA-256) convert data into an encrypted "fingerprint" that represents that data's digital signature.
- SHA-256 (for example) represents a one-way hash that means that it is impossible to reverse engineer and retrieve the underlying data in original form.
- This helps protect the data's integrity. If this underlying data is changed in any way, a new hash is generated.

Encryption, Digital Identities and Securing Trading Data (III)

DLT encryption can thus enable efficient storage and filing of documents.

Once a transaction is concluded, the hashed fingerprint represent a trusted and immutable record for a network.

Nodes within a DLT network maintain the hashed digital fingerprint of transactions rather than vast quantities of underlying trade data.

Underlying documents (e.g. a swaps contract or a warehouse receipt) may be maintained elsewhere like on a secure cloud-based system, such as a peer-to-peer, distributed file storage system.

DLT and the Custody Function

Example: Custody (I)

The custody function is essential to financial markets – and especially in derivatives.

For financial derivatives – such as options or Treasury futures – require custody of such dematerialized assets.

For commodity-related derivatives, custody involves the storage and safe movement of assets like oil, wheat or livestock.

Collateral: collateral in the form of securities or cash must be securely maintained and transferred.

Ensuring data privacy provides the basis for enhancing trust and supporting custody.

DLT can securely verify transaction data, proof of ownership and individual exposures, encrypt and create a digital fingerprint for the network.

Distributed networks can reduce the chance that any single entity possesses large swaths of information.

It can thus limit damage that might arise from a failure to a central data custodian.

Example: Custody (II)

Once identities and trade information is verified through a DLT network, trusted data can support the completion of a variety of trades.

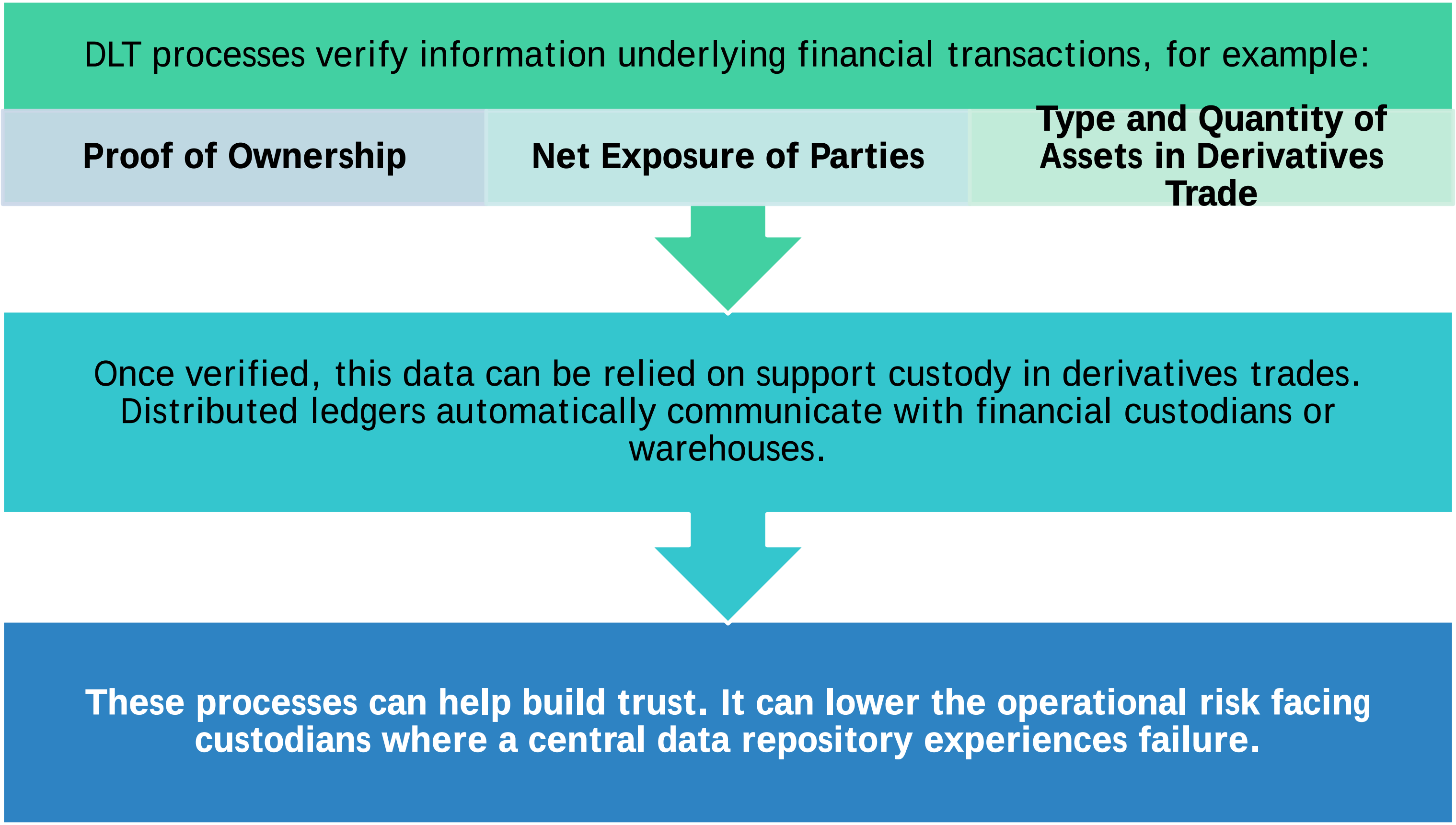
Transfer of financial assets and cash between parties (e.g. collateral management).

Ensuring that physical assets are accounted for promptly and moved between parties.

Regulators can also ensure they have access to transaction information on the ledger and where assets are located and stored.

Example: Custody (III)

DLT, Privacy and Custody



DLT processes verify information underlying financial transactions, for example:

Proof of Ownership

Net Exposure of Parties

Type and Quantity of Assets in Derivatives Trade

Once verified, this data can be relied on support custody in derivatives trades. Distributed ledgers automatically communicate with financial custodians or warehouses.

These processes can help build trust. It can lower the operational risk facing custodians where a central data repository experiences failure.

Audits, Sharing Data and Facilitating Trades

Audit and Compliance

- Financial data can be dispersed within firms
- Audit and compliance needs an indelible record of all key transactions over reporting period

DIt-based networks collect transaction records from diverse set of financial systems

Append-only and tamperproof qualities create high confidence financial audit trail

Privacy features ensure authorized user access

This can lower the cost of audit and compliance

Regulators can have “seek and find” access to data

Shared Reference Data

- Competitors/collaborators in a market (e.g. OTC swaps) need to share reference data, e.g. bank routing codes
- Traditionally, each member maintains their own codes, and forwards information to a central authority
- An information subset can be owned by organizations

Each participant maintains their own codes within a permissioned DLT network

The network can create a single view of the entire dataset to those given access to this data

Consolidated, consistent dataset reduces errors and transaction costs as well as allows near real-time access for parties and regulators.

DLT can supports code editing and routing code transfers between network participants

Concluding Trades between Multiple Parties (e.g. Letters of Credit)

- Bank handling letters of credit wants to offer them to a wider range of clients.
- Currently constrained by costs and execution times.

DLT can provides common ledger for transactions such as letters of credit

Allows all counterparties to have the same validated record of transaction and fulfillment

It can reduce transaction costs, execution times, currency fluctuation risks and improve monitoring.

Ongoing Questions for Policymakers

Do DLT-based information verification standards meet various legal standards for data privacy and security in derivatives?

For interoperability, will markets demand just a handful of encryption standards?

How should innovation in encryption take place, where a handful of standards support financial markets?

Should the CFTC lead international standard-setting in relation to data privacy and DLT?