FAC Technical Summary

FAC believe the Fund Management industry is facing a crisis, Fund Managers are seeking ways to improve performance to justify fees and charges to a changing investor community looking for better value. Part of the problem is the high cost of Fund investment compared to alternatives, largely due to the extended fund value chain made up of numerous intermediaries, each adding cost, time and risk.

The deployment of innovative Distributed Ledger Technology (DLT) provides a unique opportunity for the funds industry to achieve significant cost of operation, settlement timing, data timeliness and client service improvements.

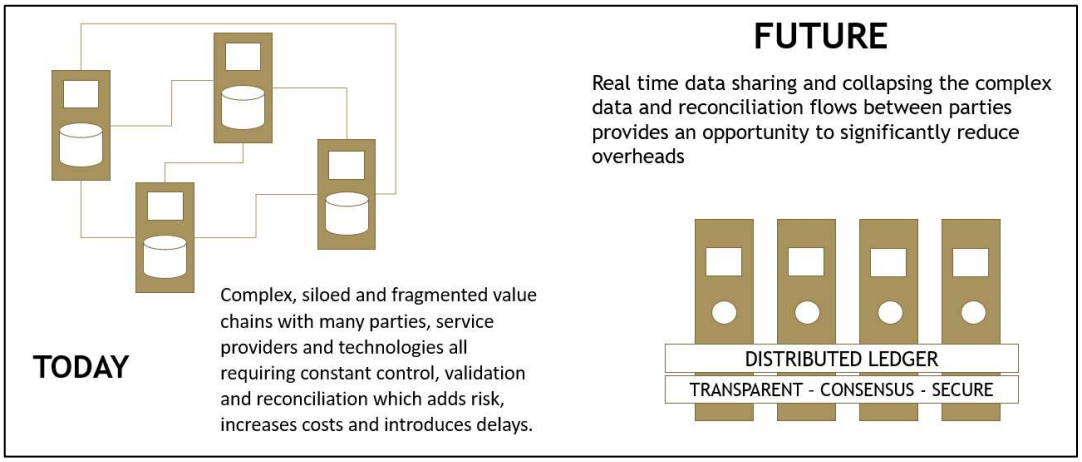
FAC are at the heart of this change, designing and building the core solution and building the network of required participants for such a collaboration to succeed.

1. What is Distributed Ledger Technology?

Until recently businesses have operated with their data and systems in silo's, constrained by organizational, process and technical boundaries. Crossing those boundaries; participating in markets, collaborating across industries and scaling globally has required complex systems to exchange and reconcile data, the need for numerous intermediaries and the formation of centralized exchanges to facilitate interoperability and provide assurance of delivery and settlement. Although highly successful at providing growth and scale this approach is grossly inefficient, costly and prone to errors.

What if data could be shared transparently, transactions completed without intermediaries and payments settled immediately? This would dramatically lower costs, collapse value chains and reduce complexity, transforming business.

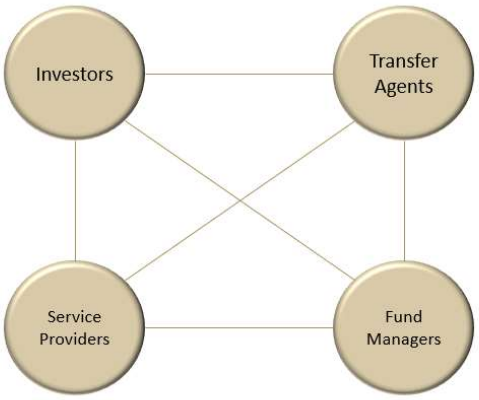
A distributed ledger is a synchronized set of data, shared across a network with multiple participants Each participant has a node on the network that allows them to share data and run applications. Security and trust in the integrity of data is maintained by use of cryptographic functions and consensus mechanisms. This creates a platform that businesses can more easily transact with each other directly without the cost and delays associated with intermediaries and centrally controlled markets.



2. A Distributed Ledger for Funds Servicing

Investors in mutual funds soon discover there is a large number of intermediaries and servicing companies that are involved in the delivery of the products provided by fund managers. Fund administrators, transfer agents, custodians and distributors all serve roles in ensuring the integrity and security of the investment process but also add significant costs, delays and complexity into the process of buying and selling mutual funds.

By bringing together the principal participants in the mutual fund value chain onto a distributed ledger data can be shared quickly, transparently and securely without the messaging and interchange costs of today's networks, reconciliation processes are collapsed and settlement can be achieved instantly. It is not just investors that benefit from this, fund managers costs are reduced, additional markets are opened up and there are new insights into cash flows and investor behavior.



In addition to the principal participants, a funds servicing distributed ledger network provides digital custody, asset custody and cash settlement, liquidity and identity services. These participants join together in a heterogeneous network that delivers a low cost, trusted and scalable platform.

The opportunity of distributed ledger goes beyond optimizing processes across organizational boundaries. As more investors and fund managers join the network competition is increased, market efficiency is improved and costs are driven down whilst regulators benefit from real-time oversight of market activity.

Central to adoption of distributed ledgers for financial products is the ability to digitally represent cash and assets on the ledger, transfer title over these assets and provide finality of settlement and conversion back into fiat currencies. This process relies on tokenization, the digital representation of cash and assets in a distributed ledger (see next section). In the near future this process is going to transform the way all financial products are produced and consumed.

3. Tokenisation

Tokenisation is the process of representing assets (cash, securities or other financial instruments) in digitized form on a distributed ledger. These tokens are digital blocks of information which are

cryptographically signed. Rather than entries in a database, these tokens are often described as like promissory notes or IOU's. Signed, immutable records of an asset which can be passed from one party to another.

On FAC Asset tokens are a digital representation of the fund share or unit. Although still a dematerialised instrument they are analogous to a share certificate and the FCA proposes to regulate them in the same way that existing shares are.

On FAC Cash tokens are a form of e-money, a digital representation of value issued on a distributed ledger that functions as a medium of exchange. The key features of the FAC cash token are:

- Provides a legal claim on the issuer
- Is valid only within FAC network
- Has a fixed 1:1 conversion with fiat currency
- Is accepted in final settlement in exchange for fund shares

4. Corda

FAC is built on the Corda Distributed Ledger Platform.

www.corda.net.

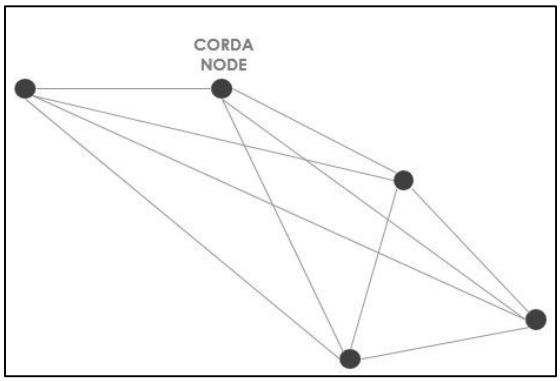
Corda was developed in 2016 by R3, an enterprise software firm, in collaboration with over 200 technology and industry partners and now has a global ecosystem of developers.

Corda is an open-source distributed ledger platform written on Kotlin which allows developers to build interoperable networks that transact in strict privacy.

The Corda platform is already being used in industries from financial services to healthcare, shipping, insurance and more. It records, manages and executes institutions' financial agreements in perfect synchrony with their peers, creating a world of frictionless commerce.

5. FAC Network Architecture

The Corda platform allows FAC to provide a specialized network for the funds servicing industry supporting order processing, registry maintenance and transaction settlement.



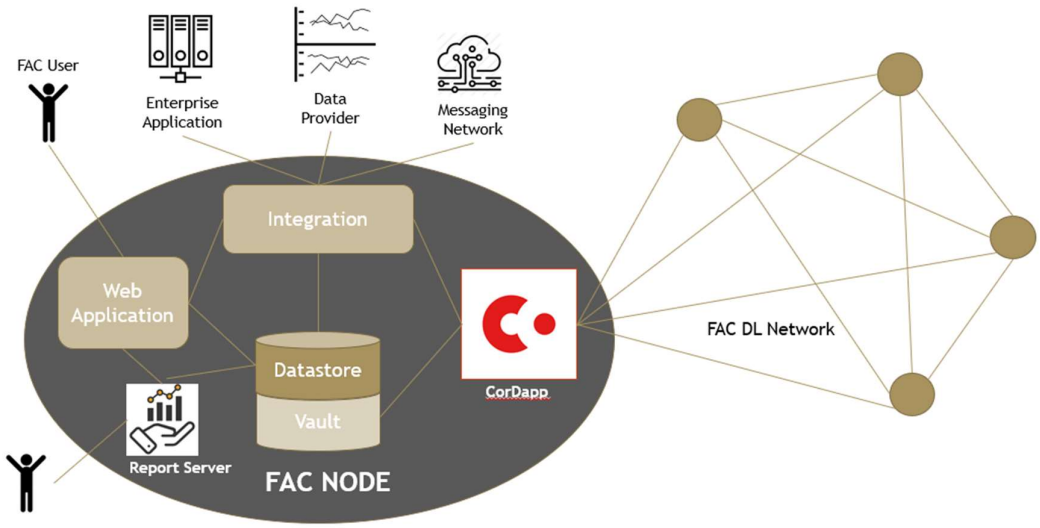
FAC is a private permissioned network where each participant on the network has its own node and with access authenticated by a certificate issued by the network operator.

Communication between nodes is point-to-point using the Advanced Message Queuing Protocol (AMPQ) over TLS.

Unlike many other blockchain solutions on Corda transacting parties and participants only see the data relevant to their role and transactions.

Node Structure

Each participant node is a multi-layer system, consisting of the distributed ledger applications, data storage, integration and web access components. A more detailed version of this diagram is in an appendix.



CorDapp and Database

CorDapp (Corda Distributed Application) is an application running on the Corda platform, and at the heart of the FAC platform.

The goal of a CorDapp is to allow the participants to reach agreement with other network participants on updates to the ledger. This is achieved by designing and implementing (on Java and/or Kotlin) following class definitions:

- States (to define the facts over which agreement is reached);
- Contracts (to define what constitutes a valid ledger update); and
- Flows (to define a routine for the node to run, usually to update the ledger).

The flows can be invoked by the node's operator using the web application or via API's .

All updates to the ledger are stored in CorDapp PostgreSQL database as immutable Corda states. At the same time some data is copied to a conventional relational data store which also holds personal information in a GDPR compliant (editable and removable) format.

Integration

FAC integration components act as the intermediary between the Web Application and the Corda application but also provide API gateways for interaction with external systems and data sources. Different levels of integration are supported by RPC, Web Socket and MQ API's.

Web Application

The FAC web application allows end-users (investors, distributors, funds and exchange administrators) to interact with the distributed application with role specific functionality to support their business processes.

Reporting

FAC uses Jasper Reports Server for reporting. It provides reporting and analytics that can be embedded into a web as well as operate as a central information hub for the enterprise by delivering information on a real-time or scheduled basis in a variety of file formats.

Network Services

Network Map Service: Corda nodes discover each other via a network map service. You can think of this service as a phone book, which publishes a list of peer nodes that includes metadata about who they are and what services they can offer. The network map service maps each well-known node identity to an IP address. These IP addresses are used for messaging between nodes.

Notary Service: A notary is a network service that provides both validating consensus and uniqueness consensus by attesting that, for a given transaction, it is both valid and it has not already signed other transactions that consumes any of the proposed transaction's input states. The notary provides the point of finality in the system.

Key Management Service (KMS): The KMS is responsible for storing and using private keys to sign things. An implementation of this may, for example, call out to a hardware security module that enforces various auditing and frequency-of-use requirements. The KMS is a node level service.

Corda Firewall: Corda Enterprise includes a component called the *Corda Firewall*. The firewall is actually made up of two separate modules, called the *bridge* and the *float*. These handle outbound and inbound connections respectively. The Corda Firewall acts as an application level firewall and protocol break on all internet facing endpoints.

For more information please contact Chris Baldwin, FAC Technology Manager, chris.baldwin@fundadminchain.com

Appendix 1 – Solution Summary

Topic	FAC Solution
Industry / Market	Financial Services / Mutual Fund Servicing
Value Proposition	Significant reduction in operating costs within the fund operations value chain through shared data, removing duplicated process as well as the need for reconciliations and messaging protocols
Primary use cases	**Launch:** Fund managers can launch tokenized funds onto the network via fund servicing nodes. **Transact:** Investors can transact with fund servicers to buy and sell tokenized shares in funds. **Settle:** Atomic settlement on ledger between investor and fund results in immediate finality. **Maintain Register:** Primary register of fund shareholders maintained on ledger. **Distribute income:** Funds can distribute income to investors with tokenized cash.
Blockchain Platform	Corda Enterprise (v4.8)
Rationale for this choice	Corda Enterprise is designed to meet the needs of financial organizations for privacy, performance and scalability. It is supported by R3 and a growing ecosystem of developers and service providers.
Development Language	Java/Kotlin
Cryptographic suite	**Node identity and network map:** Pure EdDSA using the ed25519 curve and SHA-512. **Certificate authorities and TLS:** ECDSA using the NIST P-256 curve (secp256r1) and SHA-256 (NIST recommended and HSM compatible)
Network Design	FAC is a private permissioned network
Nodes	Fund Manager (multiple) Fund Servicing (multiple) Investor/Distributor (multiple) Cash Exchange (single) Asset Exchange (single) Regulator (single) Business Network Operator (BNO) (single)
Participant Access	Participants operate their own nodes and are permissioned onto the network by the Business Network Operator.
User Authentication	FAC nodes operate a role based user access control service using an Open LDAP service.
User interaction	General access by web browser based GUI. Sone nodes can be remotely operated by API
Network Services	The BNO operates Corda generic services for the notary, network directory and network management. Third party providers will operate exchanges, KYC and digital custody services on the network
Messaging Layer	Corda uses point to point messaging instead of global broadcast. The messaging layer is AMQP/1.0 over TLS between nodes which is currently implemented using Apache Artemis, an embeddable message queue broker. Building on established MQ protocols gives us features like persistence to disk, automatic delivery retries with back off and dead-letter routing, security, large message streaming and so on.
Integration	The FAC Cordapp supports an API that allows integration to third party systems for investor servicing, token issuance and reconciliation. The FAC API layer uses an AMQP broker and HTTP calls to interact with third party systems.
Consensus mechanism	Transactions are validated by their participants and then checked by an independent network notary service to prevent double spend before

	committing to the chain. A standard Corda non-validating notary service is used. In production this will be operated by the BNO as a centralized high availability cluster using a Raft consensus mechanism.
Ledger	Unlike other blockchain solutions, in Corda there is no single block chain. Instead, each node maintains its own record of the transactions it has participated in. No node contains the entire blockchain. Corda uses a UTXO (unspent transaction output) model where every state on the ledger is immutable. The ledger evolves over time by applying transactions to change states
Value on Ledger	Both cash and fund assets are tokenized on ledger using a solution based on the Corda token SDK. FAC issues fungible tokens for both cash and assets. This supports atomic settlement of transactions providing immediate finality. Corda uses a UTXO model to represent
Smart Contracts	FAC uses Corda contracts to validate transactions. In the future there is a possibility to introduce fund specific smart contracts that enforce the dealing terms and legal contracts for fund investors.
Data Privacy	Personal information is held off chain on the investors node and syndicated on a case by case basis to other nodes permissioned to receive it.
Key Management	In production node operators will have the option of an HSM key management solution. FAC intends to support third party key management / custody solutions when these are provided for Corda.
Node technology stack	Ubuntu OS Docker container JVM (OpenJDK) Corda Distributed App (Kotlin) Apache Artemis (AMQP) PostGreSQL Database Nginx webserver (UI) Web application (Webpack/ReactJS/MaterialUI) Web Socket (Vertx EventBus) Jasper Reports Open LDAP
Database	FAC uses a PostgreSQL database. Data Schema's are directly addressable via JDBC. Corda chain data (states) are stored in a reserved section of the databased referred to as the vault. Corda uses object serialization and stores data in the database as binary objects. FAC also uses Corda Queryable states to parallel save data to SQL tables for analytical and reporting purposes.
How is resilience achieved?	Corda is built on tried and tested technologies such as Java Virtual Machine and SQL, it supports the use of commercial RDBMSs and Cloud. This makes it possible to utilise existing approaches to ensuring nodes operate with high availability and redundant capability. Should a node fail the flow framework guarantees atomicity of processing incoming events. This means that a flow or the node may be stopped at any time, even during processing of an event and on restart the node will reconstruct the correct state of the flows and will proceed as if nothing happened.
Deployment options	Container based deployment on cloud servers (Microsoft Azure). For access to the node the following firewall ports to be opened*:* 17701 - 17712

Appendix 2 – Architecture Diagrams