Corda Solution Guide

The Corda Platform
Q3 2017

Table of Contents

Introduction 3

Solution Overview 4

Needless friction hampers business transactions 4

Corda creates frictionless business 4

Benefits 4

Use cases 5

Finance *5*

Supply chain *6*

Trade finance *6*

Insurance *7*

Healthcare *7*

Government *8*

Corda Overview 9

Transact directly between parties 9

Distributed ledger *9*

Smart contracts *9*

Consensus as a service 10

Privacy 10

Interoperability 11

Enterprise Operation 14

Mission critical 14

Integration 14

Proven technologies and skills you have 14

Cloud scale 15

Join the Distributed Revolution 16

About R3 16

Introduction

Corda removes costly friction in business transactions by enabling businesses to transact directly. It enables dramatic efficiency gains in complex business operations by guaranteeing that all parties are always in sync, thereby unlocking new potential for firms to grow and transform their businesses. Using smart contract and blockchain technology, Corda allows existing business networks to reduce transaction and record-keeping costs and to streamline business operations. Corda enables an interoperable, open network that empowers organizations to collaborate and transfer value directly with trust. Corda achieves this with complete privacy in a freely available open source software platform.

Solution Overview

Needless friction hampers business transactions

Market friction makes commercial transactions less efficient. Specifically, friction can come from incorrect or forged information between counterparties, difficulties in establishing business relationships or the involvement of inefficient intermediaries. These frictions are a burden for businesses and the broader economy.

Transactions between companies require complex orchestration amongst the parties involved. Different parties must reconcile multiple systems. Further, additional institutions are often involved that are not direct parties to the transaction, adding another layer of complexity. These arrangements are necessities under existing IT infrastructures but add friction and costs to the commercial and public realms.

Internal processes can be equally inefficient, as details about transactions and assets are often recorded across multiple databases within firms. This leads to a lack of consistency and can result in low confidence about an asset's true position with the firms involved. Often, laborious manual processes are used to reconcile the data.

Corda creates frictionless business

Corda removes these frictions by enabling businesses, industry groups and other organizations to collaborate, transfer value and manage contracts directly with one another. It allows these groups to deal with each other in a peer-to-peer way without unnecessary intermediaries. Corda ensures that the information one counterparty sees is exactly what the other counterparty sees. This approach eliminates the need for systems and processes that establish the trustworthiness of third parties and their data.

Corda creates more efficient markets and reduces transaction, processing and reporting costs. The outcome is a frictionless business environment with simplified processes and systems. Corda's assurance of record immutability and provenance creates an operating environment with less risk.

Corda enables all of this using distributed ledger, or blockchain, technology. The Corda platform uses a shared smart contract to encapsulate the business logic of a transaction between organizations. Corda's unique consensus architecture assures that all transactions are valid and can never conflict, the key to delivering the promise: "I know that what I see is what you see." This is all achieved with cryptographic technologies that provide an immutable record on a shared ledger system whilst ensuring data is only received by those with a legitimate need to know – the strongest privacy assurance in the industry.

Benefits

Corda delivers three primary benefits to the businesses using it:

1. Run the business with dramatic efficiencies

Transacting directly between businesses creates new efficiencies with dramatic reductions in operational costs. Businesses gain better liquidity and capital management, fraud is minimized with verifiable linked records and time to settlement for transactions is dramatically reduced. These occur with the ability to verify counterparties and properties of transactions for risk reduction.

2. Grow and transform the business
Corda also enables new revenue opportunities. Transactions that were once out of reach for businesses now become possible. For example, a direct connection to business partners opens new markets and expands the possibilities to grow or evolve a business.

3. A platform to build upon
Corda provides a platform for businesses to work together. It is an open source technology platform, freely available today. As a component of an overall technology stack, it forms the foundation of next-generation IT infrastructure.

In operating as a shared platform, Corda enables a wide set of use cases and stakeholders. R3 is actively working with software vendors and systems integrators to deliver a broad set of solutions. Such solutions can leverage a common platform for simplicity of development and interoperability. Corda is ready to use today and is already in use by X of businesses.

Use cases

Diverse industries such as finance, supply chain, trade finance, healthcare and government can use Corda to simplify business transactions and drive efficiency. Corda has addressed some of the most complex transaction types by working closely with the highly regulated finance industry. Now, along with our partners, we are applying Corda's unique solution – a consistent shared ledger system allowing for the movement of value between organizations – to other industries.

In addition to driving efficient transactions, another popular use case for Corda is the improvement of internal processes and systems. The immutable and linked nature of the records stored by Corda can streamline auditing processes by ensuring the transparency and validity of information both within and between organizations. This global, shared set of verifiable facts enables participating organizations to:

- Automate auditing of records with the linked and immutable nature of the ledger.
- Profile risk based on shared data sets for greater confidence.
- Replace internal processes and systems with dramatically simplified processes.

Finance

The financial services industry formed the earliest and most demanding use cases for Corda. New regulations for financial services firms following the global financial crisis have imposed greater costs and compliance obligations. At the same time, the industry is facing disruption

from fintech startups and new business models that are unencumbered by legacy infrastructure.

Corda has already been applied in a variety of use cases in finance to great effect. It was designed and built in partnership with the largest financial institutions to the rigor imposed by regulators and stringent industry criteria. Corda brings dramatic efficiencies to counter the greater costs while enabling new business models even within large finance corporations.

Use cases include managing contract lifecycles such as post-trade processing of a swap or management of a trade finance agreement. Corda can facilitate these asset exchanges atomically, without an intermediary. Other scenarios include:

- Payments such as Instant Money Transfers (IMT) where banks no longer need to rely on complex and expensive nostro account relationships.
- Equity post trade where settlement can occur immediately without complex arrangements for transfer of payment and assets.
- Syndicated loans where Corda can facilitate collaboration between multiple organization in complex agreements.
- Asset rehypothecation where Corda can enable regulatory control limits in the contract and reduce settlement time.

Supply chain

Modern supply chains involve interdependent organizations that must collaborate to deliver a final product to market. Complex systems such as those producing aircraft or automobiles require the collaboration of numerous organizations with massive amounts of information and physical parts. This information forms a long, dependent chain of data that must be verifiable, trusted and immutable.

Corda provides a platform for collaboration across such chains without the need for a centralized and trusted party that can act as a single point of failure. Corda enables supply chains to:

- Show provenance of information and verify its authenticity.
- Create automated auditing and encapsulation of business rules into transactions.
- View connections such as a particular component's origin and the dependent systems that may be impacted if it proves to be faulty.

Trade finance

Organizations have to balance risks across a supply chain between organizations, and often across international boundaries. Issues such as payment, delivery, timing or currency exchanges introduce friction into a supply chain. Banks have long played a role in enabling trade by providing services to manage such risks, making bank-intermediated trade finance a key driver of global trade.

Corda enables business networks to collaborate on areas such as documentation approvals for customs, port authorities or other entities. Corda also facilitates payment and release of goods with a bank's assurance. This includes the enablement of:

- Information such as shipment documentation to be shared immutably with verifiable signatures.
- Payment to be put into an escrow contract held by the parties to the contract without an intermediary.
- Efficient use of capital as processing is automated in an assured manner.

Insurance

The insurance industry brings confidence to business operations. But the industry is plagued with manual processes that require significant paperwork and processing. The required recording and processing of information related to issuance and claims adds friction.

Corda enables automation of much of these processes by building contracts that encapsulate the business logic of the policy along with a set of verifiable and immutable information. Such contracts:

- Collect verifiable information from stakeholders to a claim.
- Provide timely payments in an automated manner.
- Reduce fraud with verifiable and immutable data.
- Increase customer satisfaction with speed of processing.

Healthcare

The healthcare industry represents a large and complex network of institutions that must manage patient data in a highly regulated and fragmented environment. The challenges include:

- Sharing data to facilitate a more comprehensive view of a patient while retaining a patient's privacy.
- Synchronizing of numerous disparate systems that hold patient data with disparate identifiers and data formats.
- Intersecting with healthcare insurers and providers who require assurance on data validity and provenance.
- Managing inconsistent and complex rules and processes.

Corda unites disparate processes, increases data flow, and reduces costs resulting in improved patient experience and outcomes. The opportunities for applying Corda to solve the systemic issues of healthcare include:

- A global network of interoperable entities that can exchange data in a secure, confidential manner while ensuring compliance to healthcare regulation.
- Framework for identity that preserves confidentiality while putting patients in control of their information across providers.
- Smart contracts for a consistent, rule-based method for accessing patient data.
- Connectivity to insurance providers to verifiable, immutable records on which to base claims in an automated process.

Government

The government can play a key role in society as a trusted intermediary facilitating efficient transactions. For example, land, mortgage or car titles are areas where government plays a central role. Such titles are managed in a fragmented set of inefficient systems that require manual intervention to facilitate transactions. They are typically exposed to risks, such as fraud or error, as they are auditable only in a paper trail.

Corda reduces the need of government involvement in transactions with immutable records and atomic transactions. Transactions have the assurance of the government issuance for title. Execution can be achieved directly between parties. This unlocks new private sector scenarios for transactions with the assurance of government backing.

Corda Overview

Corda is a unique implementation of distributed ledger technology (DLT) that is the outcome of collaboration between financial institutions and technology partners. The R3 community has designed a solution that delivers on the early promise of blockchain technology while addressing business needs for privacy and interoperability.

Corda was designed for business from the start. It has no cryptocurrency built into the platform and does not require mining-style consensus, which imposes great cost with little business benefit. Corda is built as a platform that leverages existing proven technology and infrastructure. It is designed to integrate directly into organizations' systems, facilitating a rapid deployment and a smooth transition to new processes.

Transact directly between parties

Corda facilitates direct transactions between parties. This ability removes costs by ensuring systems are in agreement and a direct transfer of value can occur. It achieves this with modern cryptographic techniques focused on two main areas: distributed ledger and smart contracts. Uniquely amongst DLT platforms, Corda uses a point-to-point design: no need for routing intermediaries or global broadcast.

Distributed ledger

The distributed ledger is a digital record stored on the systems of the parties to a financial or commercial transaction or other legally binding contract. This information is stored in the Corda Vault. Facts recorded in the Vault are authoritative in themselves, not representations of data or authority held elsewhere. Such facts are recorded and stored so they can provide proof of their status, such as ownership. Corda also stores full transaction histories, allowing for provenance and the independent verification of an assured history of a recorded item.

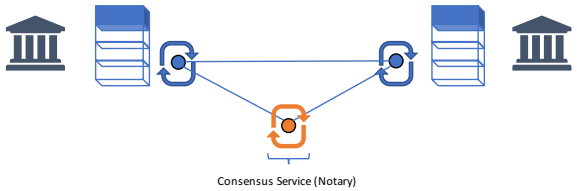
Smart contracts

The smart contract encapsulates the business logic of a transaction. It transacts on items stored on the ledgers of parties to the transaction. Contracts execute in an atomic manner, ensuring scenarios such as delivery-versus-payment occur in a manner such that both parties are assured that the inputs and outputs of the transaction transform as intended. Corda calls such contracts *CorDapps* (Corda Distributed Applications) to represent the distributed nature of the applications.

Consensus as a service

Bitcoin brought the world the ability to resolve a key aspect of a peer-to-peer transaction – uniqueness. Without this insight, transaction parties could not be confident that their transaction was not duplicated elsewhere or that it didn't conflict with another transaction that attempted to update the same record. It achieved this with its mining process, which assured parties to a transaction with multiple confirmations that the transaction could not be replaced by a conflicting transaction.

The challenge of the mining solution to uniqueness is that its finality promise is probabilistic, not absolute. Furthermore, Bitcoin's design is optimized for a world where miners are anonymous and where no party knows who any other is. This necessitates all transactions being available to all nodes in the network. This privacy leak is unacceptable to nearly all business transactions. However, Corda does not share the same requirements as Bitcoin: we require absolute certainty over transaction finality and we need to know who our counterparts are. So we had the freedom – and took this opportunity – to solve the consensus problem in a different way. In particular, Corda solves the privacy issue in a number of manners, primarily by allowing for separation of consensus into a service which we call the *Notary Cluster*.



The Notary Cluster acts as a consensus service allowing a group of servers to assure the uniqueness of a transaction. Notaries can operate in distrusted groups reaching consensus in the same manner as any blockchain system. This ensures there is no need to trust a particular party. The architecture of consensus as a service also allows for the changing of the consensus algorithm. Importantly, and uniquely, Corda can change the consensus at the point of transaction. Other systems are locked to one consensus mechanism for the business network. We currently support a simple notary and Raft. We plan to add support for Byzantine Fault Tolerance (BFT) in the near future.

Privacy

The challenge with any blockchain solution is the ability to allow for assurance over validity and integrity while ensuring privacy over transaction history. Only Corda can provide assurance over validity of a transaction and assurance that a competing, conflicting transaction has not also been confirmed in a transaction history chain while retaining privacy.

Corda achieves this through a variety of techniques. Corda's transaction history leverages and significantly extends the powerful unspent transaction output (UTXO) model derived from the Bitcoin system. This enables the 'chain' of history between transactions and forms the basis of our technical approach.

We achieve absolute privacy through:

- Full encryption of the peer-to-peer network.
- Key rotation and randomization with automatic identity management to de/anonymize transactions.
- Transactions structured in a Merkle tree allowing selective information to be revealed.
- Intel Software Guard Extensions (SGX) enclave technology allowing records that can be verified while remaining encrypted to all parties ensuring privacy.

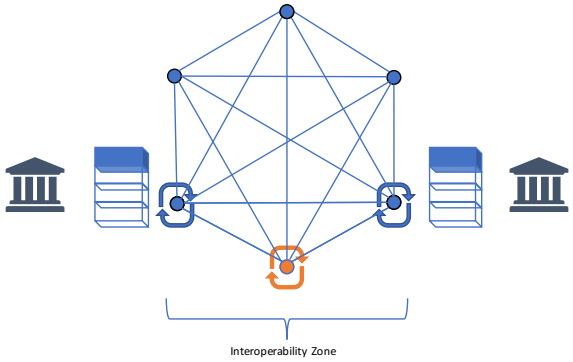
Intel SGX is a technology from Intel that places an encrypted tamper-resistant memory space into a CPU. This enclave allows trusted execution of code that is resistant to tampering and unobservable even within the computer's own execution environment. This unique technology allows for encryption of the transaction history that can only be decrypted and verified in a secure enclave. Even the Corda instance itself or the holder of the transaction history is unable to decrypt the contents.

Interoperability

Early use cases for distributed ledgers involved a small set of parties in narrowly defined transactions. We believe the end state for these systems will be a much more complex ecosystem of entities freely transacting in an open, global network.

Without such interoperability, assets will become trapped in ledgers. Cash issued by a central bank would be unable to move freely between business networks causing severe liquidity issues. Assets would be un-tradeable outside a small network of predefined entities. The goal of reducing friction would be only marginally achieved.

This same evolution in technology has occurred countless times in the past. Obvious examples include the evolution from private networks to the open internet. Or from private email systems such as Compuserve mail to internet-based email systems. The value of the network increases exponentially as its size increases.

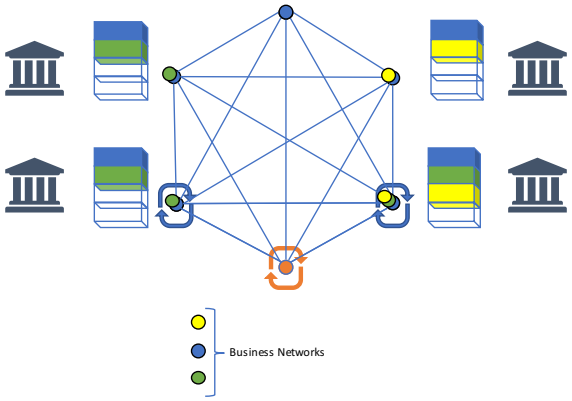


Corda operates in larger networks that we call *interoperability zones*. Such networks are able to transact between any nodes in a point-to-point manner. The root of trust in an interoperability

zone is the certificate authority's root. Corda uses this technical reality to create a global interoperability zone. Only Corda achieves this while retaining all the privacy characteristics businesses demand.

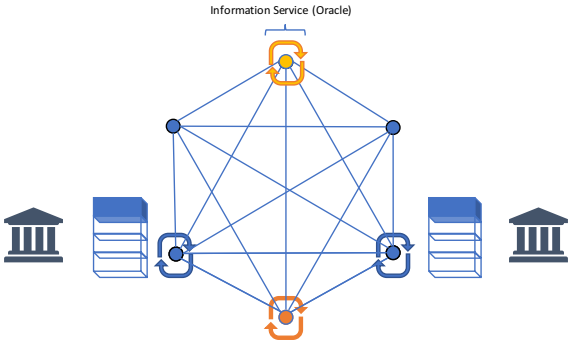
Business networks

Within these zones business networks can form to create logical groupings of entities. Such networks can be governed by a set of rules and managed by business network operators. Network operators can control membership. They can also enforce rules such as particular conditions for dispute resolution, determine what contracts are agreed upon, which notaries to utilize or other conditions that ensure conformity to the conditions of the operator.



Only Corda allows the nodes that participate in business networks to interoperate with nodes in the interoperability zone that are outside of these business networks. All other solutions trap their assets in the business networks due to the nature of their consensus mechanism and ledger design. Indeed, some solutions go even further and trap assets in *subsets* of their business networks.

Oracles - Information service providers



In this open, interoperable network, transactions will require information to be provided to them in a verifiable manner. Verifiable and immutable data allows the smart contracts to execute in a deterministic manner. Such information can be provided by operators of Corda nodes in a capacity we call *Oracles*. Oracles provide information such as interest rates,

exchange rates or any other information that forms a component of a contract. The information provided is signed ensuring the parties to the transaction can verify its source. It is immutable giving the assurance both during the transaction, and in case of later audit or dispute, that it has remained untampered. Oracles operate in a commercial manner that assures they can receive payment for their services. Oracle providers can deploy their Oracle services into one interoperability zone and service all business networks within that zone. This provides a simple way for providers to capture a large opportunity with a fixed effort.

Enterprise Operation

Corda was designed for business from the start. Business operations require reliability, uptime and integration to existing systems. Corda Enterprise is R3's commercial offering that brings enterprise capabilities to the Corda platform. Enterprise builds upon Corda's core DLT functionality to ensure availability, security and performance commensurate with the role it will play as the backbone of commercial transactions. It also adds capabilities that allow for advanced transactions.

Corda Open Source will remain a fully capable platform that is compatible with other versions of Corda such as Enterprise. Developers can remain confident that development on the open source version will run on the Enterprise version.

Mission critical

Corda Enterprise is specifically created to fulfill the non-functional needs of scenarios that are mission critical to organizations ensuring resilience and performance. Enterprise enhances these capabilities to include:

- High availability.
- Performance.
- Enhanced security.

Enhanced security includes our implementation of Intel's SGX technology for complete privacy of transaction history. This extends Corda's privacy architecture to an industry-leading position. It also includes Hardware Security Module (HSM) integration to allow enterprises to securely manage their cryptographic keys.

Integration

Corda is designed to fit into the modern data center and cloud infrastructures. It quickly integrates with existing systems and front-end processes. Such capabilities include:

- Modular database such as SQL Server, Oracle and SQL Azure.
- Modular message queue such as Artemis with upcoming support for any queue compliant with Advanced Message Queueing Protocol (AMQP) 1.0.
- Lightweight Directory Access Protocol (LDAP) and Active Directory integration.
- Existing payment and business networks and formats such as Society for Worldwide Interbank Financial Telecommunication (SWIFT) and Financial products Markup Language (FpML).

Proven technologies and skills you have

The total cost of ownership (TCO) of any solution is driven by many factors. TCO includes the landed and maintenance costs. Software license fees typically form a small component of the customized and installed solution. The key variables to lower TCO are the full stack of

technologies involved and the cost of the skills required. Corda started with a view toward a lower TCO by using a foundation of proven technologies driving a faster return on investment.

IT professionals love Corda because it uses many familiar tools and paradigms, like relational databases, the Java platform and message queues. We are able to leverage proven and well-known high availability disaster recovery (HA/DR) capabilities by using a modern relational database as our persistence store. Corda not only persists the ledger to the database but also provides checkpoints in process workflows to ensure high resiliency. Using an AMQP 1.0 system for our internode communication allows us to leverage the proven messaging systems that operate today. Corda operates on a Java virtual machine (JVM), which has years of proven operational capabilities. This is different from alternative platforms that are building new virtual machines and protocols that are not only unproven but limited in their capabilities.

Developers love Corda because they can create distributed applications rapidly using any JVM language such as Java. With over seven million Java developers in the world today it's a great way to put existing skills to work. Developer productivity is enhanced as Corda contains built-in smart contracts to facilitate interoperability on common contracts such as cash or other financial instruments allowing them to work at higher levels of abstraction. It also provides the only workflow engine to rapidly facilitate the development of complex workflows and interoperability between organizations.

Cloud scale

Corda was developed in the cloud era and is built to leverage the scale and economics provided by the cloud. With our standard architectural components such as a relational database and AMQP messaging system we can leverage the elastic managed services of the cloud. R3 is partnered with Microsoft to bring the power of Corda to Azure, although Corda nodes themselves can run on any cloud infrastructure, and is investing in deeper integration for the best offering in a managed solution.

Join the Distributed Revolution

The technology underpinning Corda will improve the processes and systems of many industries. Now is the time to take the next step with R3 to create a more efficient business and leapfrog your competition. R3 is built on partnerships and collaboration, backed by a consortium of the world's largest financial institutions. Our technology is open to you. Get started with these three steps:

Develop. Create distributed applications today. Head over to corda.net where you can grab our open source technology and access a wealth of guides to get you moving quickly.

Connect. Join Corda's vibrant community. Come learn from experts in our open forums and chat rooms at corda.net. We spend much time here so please say hello!

Partner. Leverage Corda as an open platform for enhancing your own solutions and better serving your customers with distributed ledger technology. Drop us a note at partner@r3.com to explore how we can work together.

About R3

R3 is an enterprise software company revolutionizing the way financial and commercial transactions occur with our distributed ledger technology, Corda. Distributed ledger technology (DLT), aka 'blockchain' technology, allows for not only dramatic efficiencies in the way commercial transactions occur but enables new things that haven't even been dreamed up yet. With more experience than any organization in the use and study of DLT we are creating a new future for global commerce and the finance industry.

HYPERLEDGER

R3 is a premier member of Hyperledger, a Linux Foundation Project. R3 holds a position on the technical steering committee and governing board. Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration including leaders in finance, banking, Internet of Things, supply chains, manufacturing and technology.