Corda for Business Professional Certification Exam Study Guide

R3's Developer Relations • August 2022

Index

The Corda For Business Professional Certification Exam is designed for test-takers to demonstrate a preliminary understanding of Distributed Ledger Technology (DLT), Blockchain, Corda, its business impact, and real-life applications. This exam is suitable for business professionals working with the blockchain and related ecosystems.

What is Corda?

Corda's development framework enables the building of future-proof apps quickly in financial services and other regulated markets.

Privacy

Corda shares data only between the counterparties of a transaction. Even the communication protocol itself is invisible to the other members on the network.

Development

Smart contracts are legally bound and written in any JVM compatible language, taking advantage of the vast ecosystem of tooling and libraries.

Regulator Compliance

Corda capabilities are grounded in legal constructs and compatible with existing and emerging standards and regulations.

Scalability and Sustainability

P2P architecture enables high levels of network scalability and throughput. Transactions don't need to be sequential, increasing the overall efficiency of the system. Approximate energy or joules consumed per transaction: 24.6.

Settlement

Consensus model guarantees that assets have deterministic settlement finality because it is based on validation and uniqueness.

Security

In order to participate in a CorDapp each entity must be granted access to do so and tied to a legal entity.

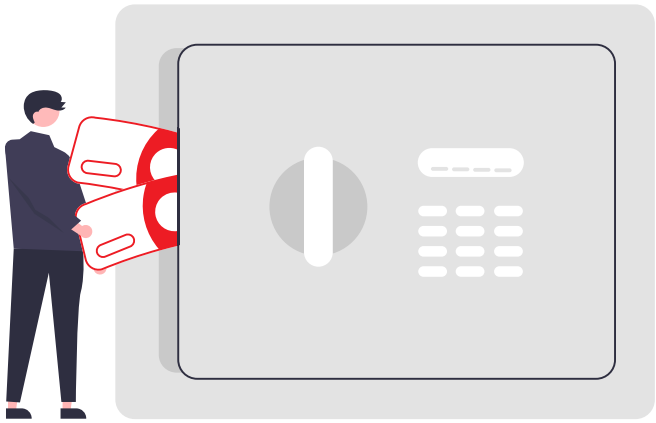
Blockchain/DLT Fundamentals

Blockchain (often referred to as Distributed Ledger), are blocks of transactions chained together across a shared ledger using cryptography. Blockchains solve Byzantine generals problem and double spending.

Private blockchains such as Corda are purpose-built to improve the existing interactions of firms in a market by improving efficiency, optimizing processes, eliminating duplication, and increasing certainty. We take ideas from the public chains and apply them to the most challenging problems faced by regular businesses.

Corda is being used by some of the largest financial institutions in the world to create regulated, trustworthy networks. This enables customers to safely hold, trade and innovate with digital assets of any type, whether they be traditional, natively issued on Corda, or assets from public blockchains that have been immobilized and bridged into the regulated perimeter.

Public blockchains have permitted an entirely new way of transacting with each other: permissionlessly. Thanks to these innovations, you don't need permission to create a new natively digital asset on a public blockchain, and you don't need permission to transfer such assets to anybody else. Public blockchains don't allow for both public and private transactions on the network. In public blockchains all parties in the network have a replica of the ledger and identities of other parties are unknown in a public chain.



The distinction between Public and Permissioned is based on the criterion for entry to the network.

Analyzing and determining the right use case is the first most key step towards developing a blockchain solution. When choosing what blockchain to use, these factors play a vital role in the decision-making process:

- The number of participants involved
- The importance of record-keeping compliance and reconciliation
- The need for the transfer of digital assets and payments

Corda and Hyperledger Fabric are permissioned blockchains. Not all blockchains come with a native cryptocurrency.

Distributed ledger technology closely relates to distributed database. Oracle and SQL Server are databases supported by Corda. The database used in a development network is H2. Keep in mind that data needs to be backed up by each participant.

AMQP (Advanced Message Queueing Protocol) is Corda's P2P messaging protocol.

Applications built on blockchain are called:

- **Dapps** – decentralized applications
- **CorDapps** – Corda Decentralized Applications
- **Smart Contracts** – governs how transactions happen between parties. Java and/or Kotlin can be used for developing Smart Contracts in Corda. Note that Bitcoin doesn't support Smart Contracts.

You don't need a blockchain network when parties trust all the other parties in the network. An Internet connection is required to connect to a blockchain network.

Cryptography

Cryptography is one of the key technologies that form the backbone for any blockchain.

Hashing, public and private keys, and digital signatures are cryptographic techniques used in Corda.

Cryptographic hashing converts an arbitrary length of text to a fixed length of data that acts as a unique identifier for the data.

Public and Private keys

The user generates a pair of keys that are used for encryption and decryption. These keys always come in pairs and each key offers various capabilities.

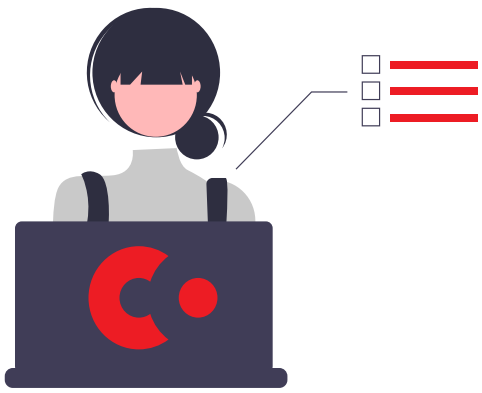
Private keys can be ideally protected using Hardware Security Modules (HSMs), desktop crypto wallets, and mobile/web crypto wallets.

Encryption of any data to be secretly sent to a party is performed using that party's public key. The private key should be kept secret. Private keys can't be derived back from the public keys.

Corda Architecture and Key Components

Corda is a permissioned "distributed ledger" coupled with a workflow messaging network. It was originally built with regulated financial institutions in mind.

Corda is a platform for creating interoperability in enterprise settings. Its impressive scalability, transaction privacy, state consistency, and workflow flexibility are suitable for a wide variety of enterprise settings including capital markets, trade finance, digital identity, insurance, healthcare, government, supply chain, and telecommunications.



In Corda, the single source of truth is visible to all required parties on the network. Information is shared in Corda on a peer-to-peer basis.

CorDapp

CorDapps (Corda Distributed Applications) are distributed applications that run on the Corda node. CorDapps allows network participants to define their custom assets, define rules that govern the modification of those assets, as wells as custom workflows to perform business processes. The goal of a CorDapp is to allow the nodes to reach agreement on updates to an asset on the Corda ledger.

A typical CorDapps has 3 major components:

1 **States** 2 **Contracts** 3 **Flows**

- **States –** a state is an immutable object representing a fact known to one or more Corda nodes at a specific point in time. A state is a fact known by one or more parties.
- **Contracts –** a contract in Corda represents the sets of constraints that govern the evolution of the state objects.
- **Flows –** helps to automate the process of agreeing on ledger updates. A flow is a sequence of steps that tells a node how to achieve a specific ledger update, such as issuing an asset or settling a trade. The flow framework in Corda guarantees eventual finality. Suspended flows are never deleted.

Corda Network

A Corda Network is a peer-to-peer network of nodes. Each node represents a legal entity, and each runs the Corda software.

The Doorman, Notary, and Network Map are services that must run in a Corda network. In Corda, user-facing client and external integration into the node is done via CordaRPCClient.

- **Doorman** – handles the management of network membership.
- **Notary** – maintains a key map of input states and the transactions that consumed them. Notary clusters prevent “double-spends”.
- **Network Map** – used to look up other nodes on the network.

A Corda node is an entity in a Corda network that usually represents one party in a business network. One party operates the node, which contains the CorDapps that the party uses to interact with other peers on the network. A node could have several CorDapps running at a given time. Nodes get accepted to the Corda network when admission is approved by the Doorman of the network. TLS is used to encrypt communications between nodes. All Corda nodes run in a JVM.

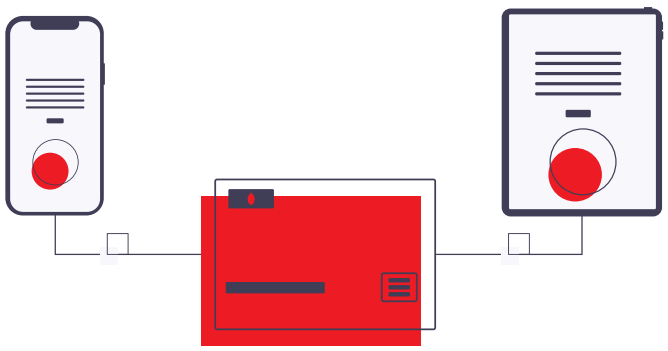
Transactions

A transaction in Corda represents a proposal for a number of participants to update their ledgers. Any party on the network can propose a transaction in Corda. Only one notary is allowed in a transaction. A transaction is only accepted when all required parties have signed the transaction. The number of participants in a transaction is unlimited.

A transaction could create zero or more output states and could be broadcasted to the Corda network. A transaction is filtered to provide advanced privacy by hiding certain components of the transaction from users who do not need to see them. A transaction can be broadcasted to the Corda network. There is a no transaction fee required to add transactions to a Corda network.

Nodes get time window signatures to prove a transaction happened before, during, or after a specific time. The notary timestamps and notarizes at the same time, so if the node doesn't need to commit to the associated transaction, it can reveal the time window in the future.

An Oracle provides data external to the ledger into a transaction and signs the transaction. Oracle services can be used both when proposing and when verifying transaction.



Consensus

Corda provides a pluggable consensus. There must be consensus that a proposed transaction is valid before you can add it to the ledger. Blockchains use consensus mechanisms to achieve agreement, trust, and security across decentralized networks.

Proof of Work and Proof of Stake are probabilistic consensus protocols. Mining is a term used to refer to Proof of Work consensus algorithms.

When the transaction has no input states and no timewindow a notary is not required to notarize a transaction. The entire historical chain doesn't have to be traced backward and re-verified in order to validate a transaction. Corda doesn't have strict consensus policies that inhibits any variation with the consensus algorithms.

Notary cluster prevents double spending in Corda. Notary cluster may be validating or not validating. In case-of non-validating notaries, it will only access the state references and doesn't need to validate the full contents. The different notary clusters that are in the same network doesn't have to run the same consensus algorithm. Many notary clusters can co-exist on the same network.

Each notary maintains a list of state references that have already been consumed to ensure each output state is only consumed once.

Token SDK

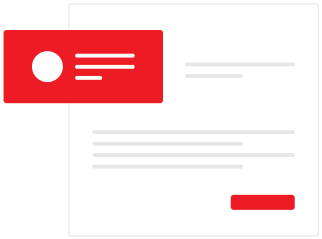
The Token SDK provides you with the fastest and easiest way to create tokens that represent any kind of asset on your network. This asset can be anything you want it to be - conceptual, physical, valuable or not. You can create a token to represent something outside of the network, or something that only exists on the ledger - like a Corda-native digital currency.

Token SDK can be used to issue fixed, evolvable as well as fungible and non-fungible tokens (Fungible tokens are tokens that can be split and merged. The smallest unit of any fungible token is always a non-fungible token).

Accounts Library

The Corda Accounts Library allows a Corda node to partition the vault — a collection of state objects — into a number of subsets, where each subset represents an account. In other words, the Corda Accounts Library allows a Corda node operator to split the vault into multiple "logical" sub-vaults.

Accounts are created by host nodes, which are just regular Corda nodes. Hosts can create accounts for a range of purposes, such as customer accounts, balance sheets or P&L accounts, employee accounts, and so on. The accounts of a node are not registered on the network map of the network.



Attachments

There are cases where network participants need to reuse a certain piece of data. Corda facilitates that task by allowing to add that piece of data as an attachment to the transaction. When a party receives that transaction, they can then request the attachment file from the sender.

Contract attachments is used to share documents with the network, on a need-to know basis.

Attachments are intended to be reused across transactions. They are stored in JAR files and presented as hashes of the original files inside a transaction.

When a node sees an attachment it resolves it by retrieving the attachment from its own storage or requests it from the counterparty. The receiver node downloads the physical files via RPC client calls.

Hashes of the original files in attachments are included to the transaction. Attachment metadata can be queried in the vault.

Aside from the type of file attached, attachments can be grouped into 2 major logical groups: Contract jar files and general files.

Use Cases

Trade finance is a set of financial tools that help with bridging the trade cycle funding gap. Consumers are never a party in trade finance life cycle. In trade finance, EBL means Electronic Bill of Lading. The risks associated with trade finance are: payment, country, and corporate risk.

80% of world trade relies on trade finance, as per the World's Trade Organisation.

Supply chain is a network between a company. Its suppliers, and distributors produce and distribute goods. In supply chain, the material flows in the forward direction and the money flows in the onward direction.

Lack of transparency, lack traceability, and absence of end-to-end visibility are some of the drawbacks of the traditional supply chain process (compared to a blockchain powered solution).

Letter of credit is used by the exporter to generate credit after goods delivery and before invoice payment. Letter of credit is issued by the Importer's bank to the exporter's bank.

Corda provides private but interoperable business network with transferable assets in contrast to other blockchains. This is extremely important while developing Cross-border payments with Corda.

Token SDK could be used for the issuance of digital currency and stocks on the Corda network and accounts SDK could be used by a bank's node to issue identities to its customers on the network.

Government is a candidate participant in innumerable Corda networks where industry requirements include notifying a regulator or a registry. Corda addresses this concern well since notifying a regulator was a primary concern of the regulated financial services industry. Analogues are found in land titles, vehicle registries, licensing and, indeed, regulation of all kinds. Each use-case has strict requirements in terms of confidentiality, public disclosure and privileged access. **Corda is a natural method of codifying process flows that ensure regulatory compliance and accurate records.**

Recommended resources to assist with certification

Corda training: training.corda.net

Documentation: developer.r3.com/docs/

Blogs: developer.r3.com/blog/category/corda

Videos: developer.r3.com/videos

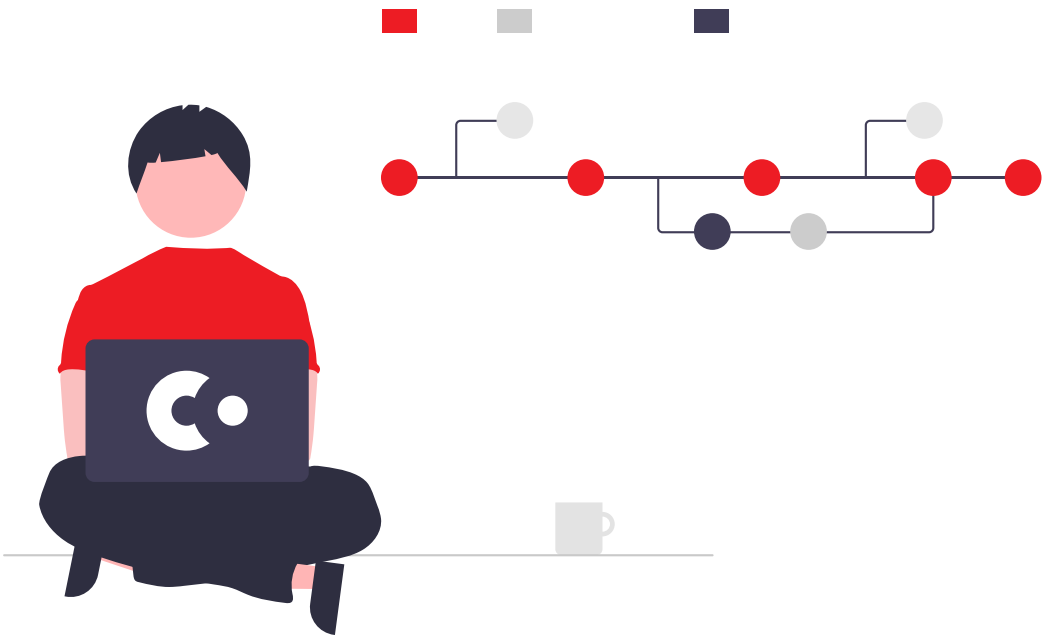
Community: community.r3.com

Open-source code repository: github.com/corda/corda

Open-source CorDapp sample repository: github.com/corda/samples

Public Slack: slack.corda.net

Good luck and happy coding!



R3 is a leading provider of enterprise technology and services that enable direct, digital collaboration in regulated industries where trust is critical. Multi-party solutions developed on our platforms harness the "Power of 3"—R3's trust technology, connected networks and regulated markets expertise—to drive market innovation and improve processes in banking, capital markets, global trade and insurance.

As one of the first companies to deliver both a private, distributed ledger technology (DLT) application platform and confidential computing technology, R3 empowers institutions to realize the full potential of direct digital collaboration. We maintain one of the largest DLT production ecosystems in the world connecting over 400 institutions, including global systems integrators, cloud providers, technology firms, software vendors, corporates, regulators, and financial institutions from the public and private sectors.

For more information, visit
www.r3.com and developer.r3.com

r3.com • developer.r3.com