Corda for business

R3's Developer Relations • Divya Taori • November 2021

Index

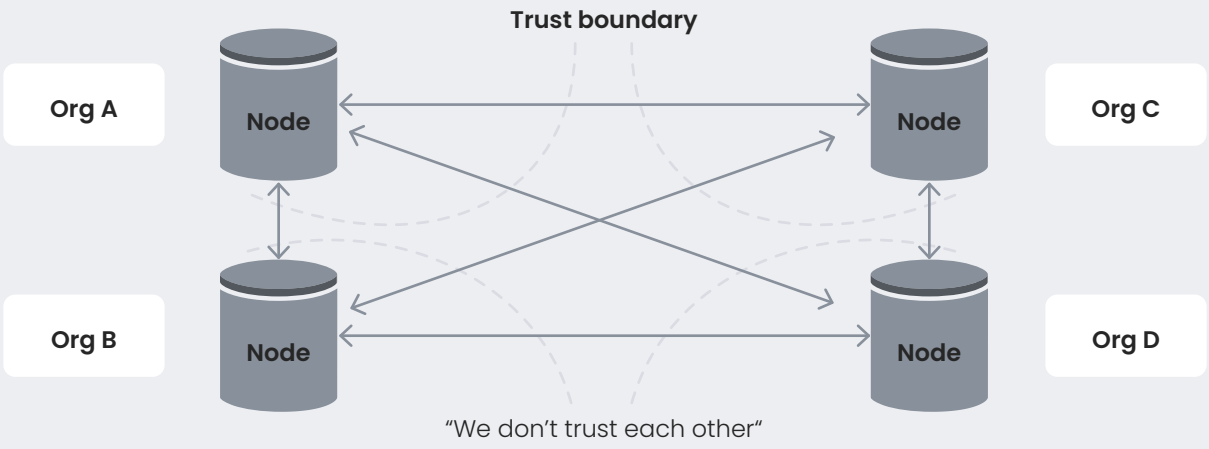
Corda is a scalable, permissioned peer-to-peer (P2P) distributed ledger technology (DLT) platform that enables the building of applications that foster and deliver digital trust between parties in regulated markets. Unlike traditional blockchain Corda has a permissioned network with legally identifiable counterparties and strict transaction finality built in.

Introduction to Distributed Ledger Technology

Distributed Ledger Technology (DLT) refers to the technology that allows several participants to record, share and maintain the information stored across multiple databases. These participants don't fully trust each other and would often consider all other parties in the network as adversaries. Even with such a trust model, the technology allows for a seamless view and update of the storage. The participants will form a consensus about each update that happens and will agree upon the state of the database. The information storage is often referred to as "shared facts."

Distributed ledgers are systems that enable parties who do not fully trust each other to form and maintain consensus about the existence, status, and evolution of a set of shared facts.

Along with storing the current state of the database, the technology also allows for participants to view a detailed log of all updates that have happened to the database. The participants, each have their copy of the shared database and are referred to as "nodes" in the network. The technology ensures that they all see the same view of the database. **DLT technology enables everyone involved to know with certainty what happened, when it happened, and confirm other parties are seeing the same thing without the need for an intermediary providing assurance and without a need to reconcile data afterward.** The below diagram explains the overall view in a visual form. The nodes would belong to different organizations/companies which don't trust one another.



Thus, the key features of Distributed Ledger Technology are:

1. **Decentralized and Distributed:** No one owns the entire network. There is no need for a trusted third party or centralized authority to provide assurance about the data of the ledger. The network is distributed, i.e., there is no administration facility or central storage.
2. **Consensus**: The parties form a consensus about the updates that happen to the ledger.
3. **Cryptography:** Ensures protection of sensitive data and identity on the DLT. It guarantees the immutability of updates that happened to the ledger, thus providing trust.

What is blockchain?

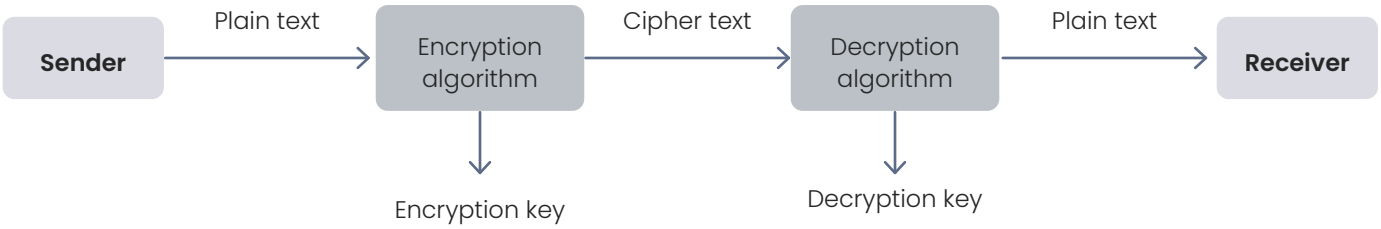
When these transactions which append the database are grouped together in blocks, with one block linked to another using cryptography, it is called Blockchain. To keep things simple, the terms blockchain and DLT have been used interchangeably in this document.

Cryptography

Cryptography is one of the key technologies that form the backbone for any blockchain. To understand the functioning of any DLT/blockchain, one must understand the basic concepts such as encryption, decryption, public, private keys, hashing, digital signatures, etc.
Though many other cryptographic concepts may find applicability in the blockchain ecosystem, this section will cover the basics and the most important principles relevant to Distributed Ledger Technology.

Encryption / Decryption

A cryptosystem refers to the implementation of cryptographic algorithms and their accompanying infrastructure used to provide information security services. It is also referred to as cipher-system. The main idea is that the cryptosystem helps convert the plaintext to ciphertext and back, thus encode and decode messages securely. When two parties communicate with each other to transfer a message (referred to as plaintext), the message is converted into an apparently random text (referred to as ciphertext). This process of converting plaintext to ciphertext is called Encryption. Once the ciphertext is produced, it may be transmitted over the network. Upon reception, this ciphertext is transformed back to the original plaintext using the process of Decryption.



The main components of a cryptosystem are:

- **Plaintext:** The message data that is to be protected during transmission.
- **Encryption algorithm:** Mathematical algorithm that converts the plaintext into the ciphertext using the Encryption key. This cryptographic algorithm takes the plaintext and Encryption key to produce the ciphertext.
- **Ciphertext**: This is the text produced by the Encryption algorithm from the plain text. It is not protected and is transmitted directly on the communication channel. Any adversary having access to the communication channel can intercept this.
- **Decryption algorithm:** Mathematical algorithm that recovers the plaintext from the ciphertext using the decryption key. This essentially reverses the encryption algorithm and is mathematically related to it.
- **Encryption key:** This key is known to the sender, who passes it and the plaintext as input to the Encryption algorithm in order to compute the ciphertext.
- **Decryption key:** This key is known to the receiver, who passes it, and the ciphertext as input to the Decryption algorithm in order to compute the original plaintext.

There are two types of cryptosystems based on how encryption and decryption are performed:

1. **Symmetric key encryption:** Here, the same key is used for encryption as well as decryption. The popular examples are Digital Encryption Standard (DES), Triple-DES(3DES), and IDEA.
2. **Asymmetric key encryption:** Here, different keys are used for encrypting and decrypting the information. Though the keys are different, they are mathematically related. It is also known as Public key encryption.
   Below, we will look more into Asymmetric key encryption.

Public key / Private key

This refers to Asymmetric Key Cryptography. 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. Those capabilities are based on cryptographic mathematics. As their name suggests, the public key

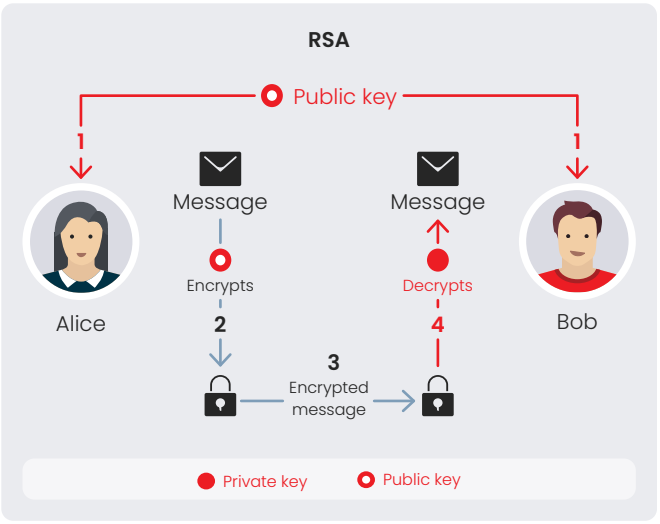
is meant to be distributed to whoever is relevant, while the private key is to be jealously guarded, akin to having your house address public, but keeping the key to your house private.

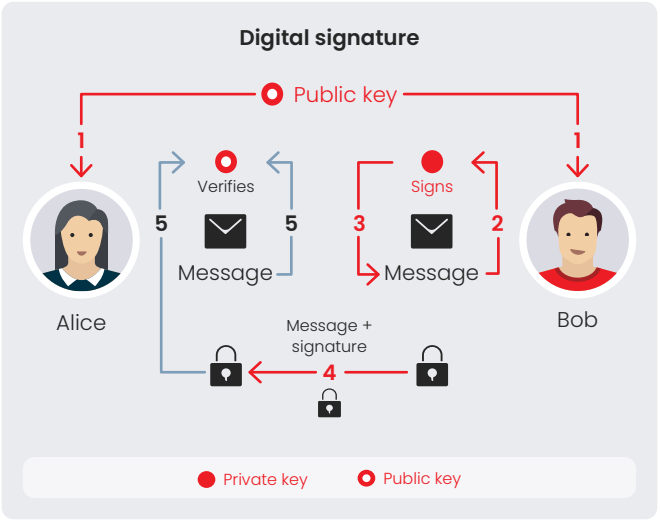
Either of these two related keys can be used for encryption, with the other one being used for decryption.

Encrypt and decrypt

Alice wants to send a message to Bob, and for Bob's eyes only:

- Bob gives Alice his public key
- Alice uses Bob's public key to encrypt the message
- Alice sends Bob the encrypted message
- Bob decrypts the message with his private key





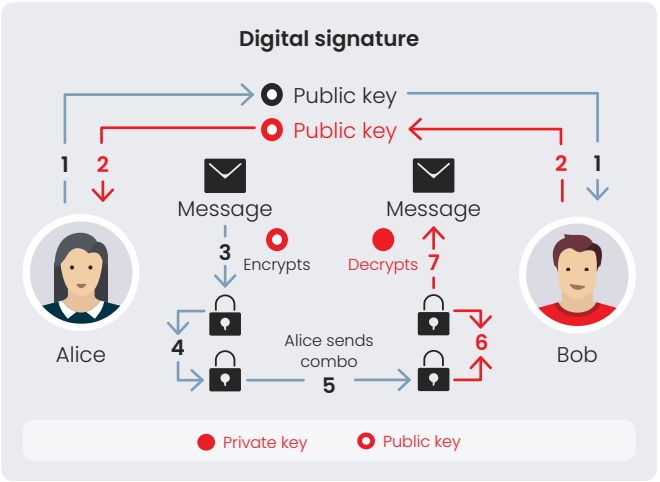
Sign and verify

Alice to make sure that Bob's public announcement is indeed from Bob:

- Bob gives Alice his public key
- Bob signs his announcement with his private key
- Bob sends Alice his announcement and its signature
- Alice verifies the signature with Bob's public key

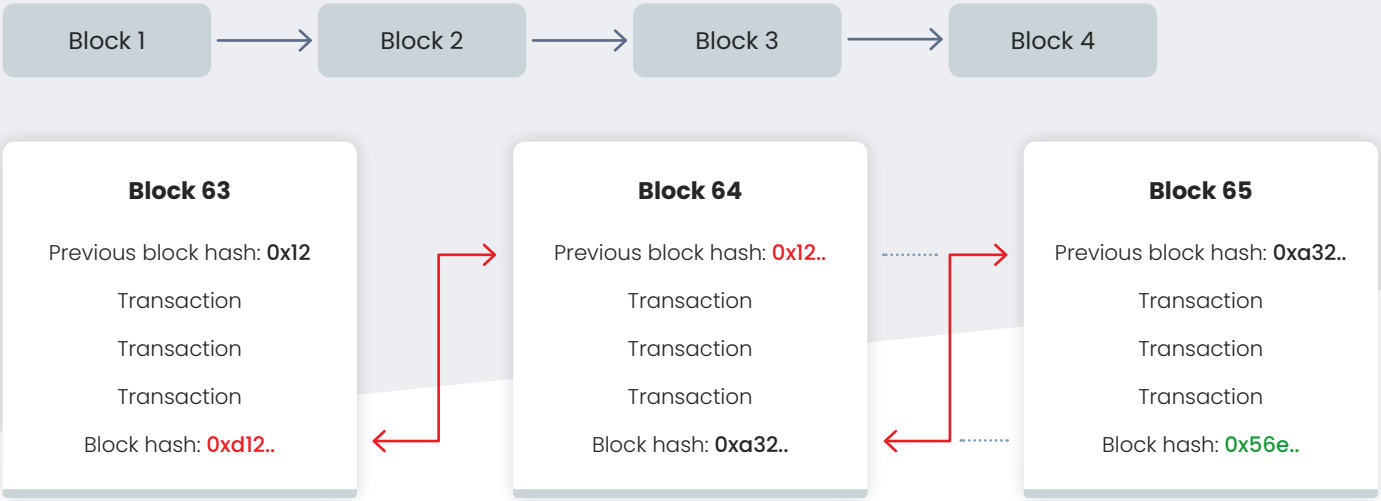
Mix and match

It is possible to mix both ideas, whereby Alice encrypts her message with Bob's public key, then signs the encrypt file with her private key. Upon reception, Bob verifies the signature with Alice's public key, then decrypts the file with his private key.



Cryptographic hash function

Hash functions convert the input to an output called the hash, such that it is practically impossible to re-generate the message out of the hash. This conversion is done quickly in a reasonable amount of time. Another important property of the hash generated is that even the tiniest change in the message changes the hash beyond recognition. Also, it is practically impossible to find 2 different messages with the same hash. In the case of blockchains, a hash is generated out of each block and any new block contains a reference to the hash of the last block.



Another crucial point to note here is with such a hash function, you can:

- Prove that you have a message without disclosing the content of the message, for instance:
  - To prove you know your password.
  - To prove you previously wrote a message.
- Rest assured the message was not altered.
- Index your messages.

Example

Bitcoin uses 'SHA-256`. Ethereum uses `Keccak-256`and `Keccak-512`.
It is possible to index content by its hash, in essence creating a hashtable. If you have used IPFS (InterPlanetary File System) or BitTorrent's magnet links, among others, then you have used a hashtable.

Digital certificates

Digital certificates are used (among other things) to prove identity. They are given by a

recognized Certification Authority (CA). A widespread procedure is the public key certificate. It proves the ownership of a public key. Below, the X.509 standard is described.

The X.509 standard is defined by the Telecommunication Standardization Sector (ITU-T) of the International Telecommunication Union (ITU). It offers format and semantics for public-key certificates. X.509 is profiled in the formal language ASN.1. Common use cases are validation of documents and securing of communication. For example, X.509 is used in TLS/SSL. Its origin is in the X.500 standard issued in 1988. Since version 3, X.509 enables flexible topologies, like bridges and meshes.

A X.509 certificate contains information such as version number, serial number, signature algorithm, validity period, subject name, public key algorithm, subject public key, certificate signature algorithm, certificate signature, and extensions. An extension has a type, a corresponding value, and a critical flag. Non-critical extensions are only informational.

Signature

The concept of digital signatures is simple. If a given message is first hashed and then encrypted by a private key, one can verify the signature by decryption with the corresponding public key. You need to hash the message to avoid the creation of signatures by mixing the messages and corresponding signatures. This way, you know that the sender has the private key to the given public key. However, this is not truly an identification. Here comes the CA. The CA signs a certificate to prove the identity of the owner of a public key. The certificate includes, as described above, the subject name. This must be verified by the CA. So, the identity is given, if one can verify the CA's signature and trust the CA.

Public and permissioned blockchains

With the increasing awareness and adoption of DLT, the blockchain evolution has witnessed the development of many new distributed ledgers and blockchains. The popular ones being Corda, Bitcoin, Ethereum, etc. All these DLTs could be categorized into 2 broad categories:

- **Public:** A public blockchain is permissionless. Anyone can join the network, read, and write to the ledger. There is no need for KYC and identity checks to join the network. All one needs is the client software to connect to the blockchain. All nodes have the same authority over the network. As malicious users could easily join the network, the blockchain would require strong implementation of crypto-economic incentives. For example, Bitcoin and Ethereum.
- **Permissioned:** A permissioned blockchain has access control, which restricts new

parties from joining the network. Only authorized nodes are allowed to participate and control the network. Such blockchains are also referred to as private chains. Most permissioned blockchains have a component that grants access to new nodes, often called Doorman.

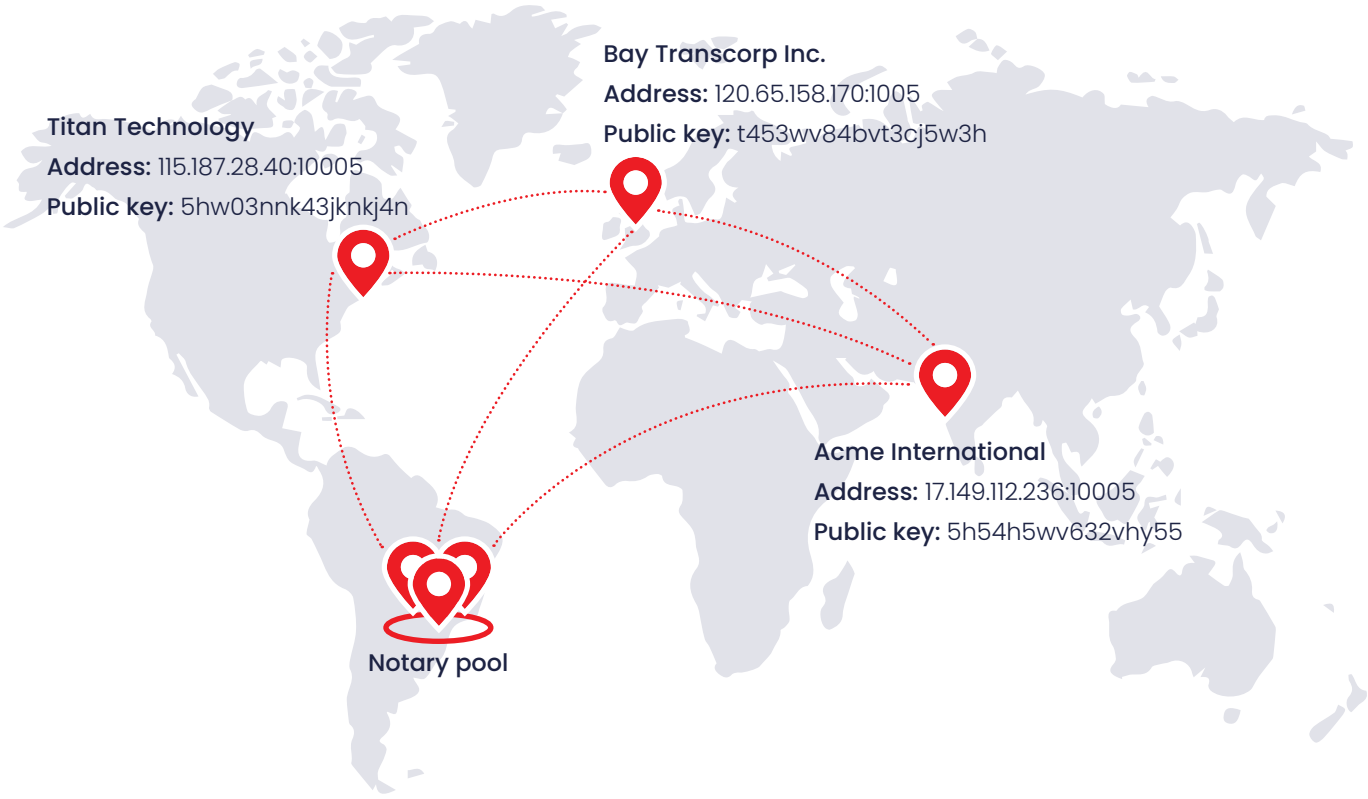
As parties are known to each other, the need for a strong underlying crypto-economic model is greatly reduced. For example, Corda, Hyperledger Fabric, Ripple.

Introduction to Corda

Corda is an open-source DLT (Distributed Ledger Technology) platform that enables businesses to transact with strict privacy with one another. Unlike traditional blockchains, Corda has a permissioned network where all participants are legally identifiable. The platform has a strict transaction finality.

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.



All communication between nodes is **point-to-point** and encrypted using transport-layer security. This means that data is shared only on a **need-to-know** basis. There are no global broadcasts. As an example, if we have a transaction involving a vehicle between Titan Technology and Bay Transcorp Inc. shown in the image above, once the transaction is successfully completed, the information of the vehicle will only be available with the transacting parties (i.e. Titan Technology and Bay Transcorp Inc.), while Acme International will no information about the transaction or the vehicle, even though he is part of the same Corda Network.

Corda Network is a permissioned network, to join a network the organization (who wants to run a Corda node) needs to obtain a certificate from the network operator known as doorman. The doorman is the root certificate authority of a Corda Network, and thus certificates of all network participants must be signed by him. The certificate is used to map an entity to a real-world legal identity and a public key. To obtain the certificate an entity must go through a KYC as defined by the governance model of the individual network. Thus, **every node is the network has a real-world legal identity, not just an anonymous public key.**

Network map

A network map is a dictionary containing the public information of all participant nodes of a network. It allows network participants to discover each other. The network operator (or doorman) is responsible for updating the network map when a new participant in onboarded or offboarded on the network. The network operator run a network map service which the participant nodes can poll from time to time to get the most updated version of the network map.

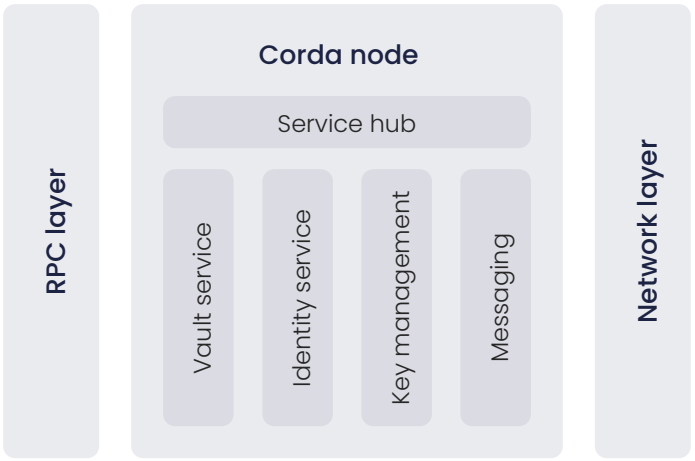
Corda node

A Corda node is a JVM runtime which is run each participant in the Corda Network. It has a unique network identity. Multiple applications called as CorDapps (Corda Distributed Applications) can be installed on the nodes. These applications contain business logic and workflows which helps network participants to perform day to day transactions.

Each Corda node has a keypair which is used to sign transaction for the purpose of providing agreement to a transaction which eventually updates some information on the Corda ledger.

The Corda node is like a black box which abstract away various complex task such as key-management, storage, identity, messaging etc. It provides various simple interfaces which the

node operator (owner) could use to issue commands to the node to run a transaction or query data from the node's vault (ledger).



The Corda node has two interfaces with the outside world:

- A network layer, for interacting with other nodes in the network
- RPC layer, for interacting with the node operator (owner)

Corda notary

Notary is a very important component of a Corda Network. It helps prevent double spending of assets in the network. It also serves as a timestamping authority of transaction happening within a Corda Network. Notary provides finality to a transaction; a transaction is considered to be completed only after it is signed by the notary.

A network could choose to run multiple notaries, and the participants are free to choose which notary they want to use for a particular transaction. For each notary identity in a Corda Network there is an option to either run a single notary node or a pool of notaries (called as HA Notary/ Notary cluster). The notary nodes within the HA (High availability) notary cannot be individually reference since they have a single unique service identity. Corda has pluggable consensus for HA notaries allowing notary clusters to choose a consensus algorithm based on their requirements.

Single notary node

Notary cluster

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.

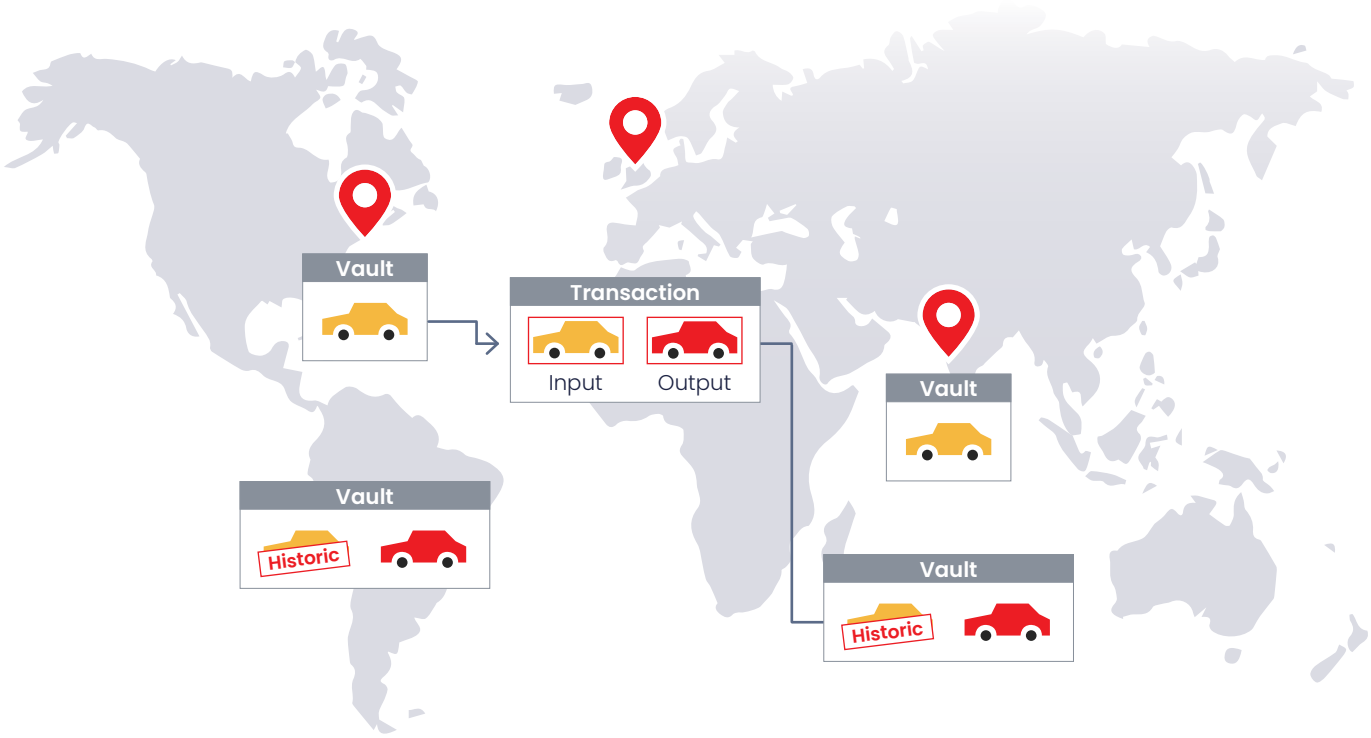
CorDapps are installed as jar file in the Corda node, and they can be written in any JVM language. A typical CorDapps has 3 major components:

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. States are used to model shared assets that are needed to be stored on the Corda ledger of one or more Corda nodes. States are shared among Corda nodes on a need-to-know basis. Thus, there is no central ledger and not all states are known to all node, this is how the entire privacy model of Corda works. However, when two or more nodes share a particular fact (or state), Corda makes sure that the copy of the state shared by each node is completely identical.

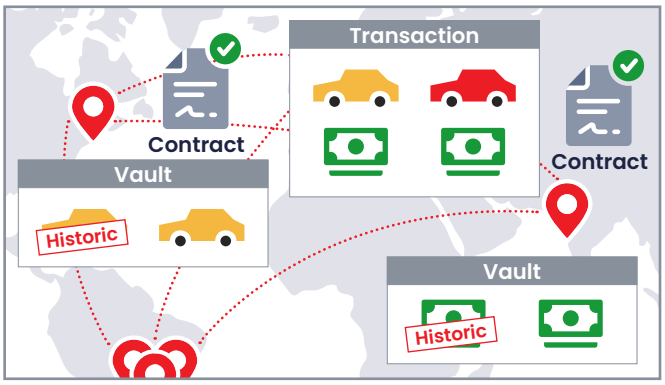
States are immutable, which means once created they can't be modified. When a state is needed to be updated, a transaction is created which updates the state by creating a new copy of the state containing the modified values and marking the existing state as historic (or spend).

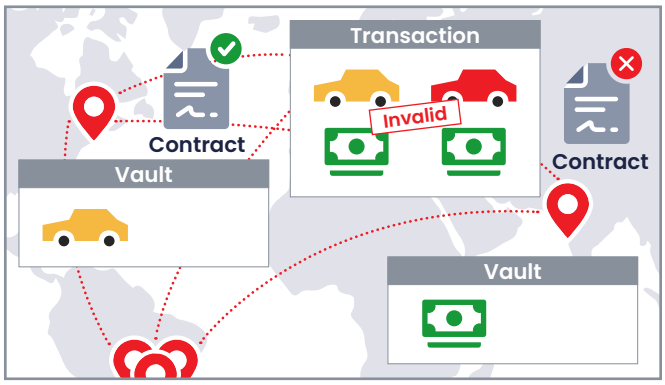


Contracts

Contracts define business rules which governs evolution of a state in Corda. A transaction is only valid if it is digitally signed by all required signers and the signers need to verify if a transaction is contractually valid before digitally signing it.

Contracts help provide validity consensus in a Corda system. Recall that notary prevents double spend (i.e., it checks for uniqueness), thus providing uniqueness consensus. However, notary (non-validating) doesn't check the content of the transaction and hence has no idea if the content of the transaction is valid. It's the responsibility of individual signers of a transaction to validate the transaction's content and verify the contents of the transaction. A transaction is said to be valid only if all the required signers of the transaction have successfully validated the contractual validity of the transaction by running the contracts installed at their node.





Commands

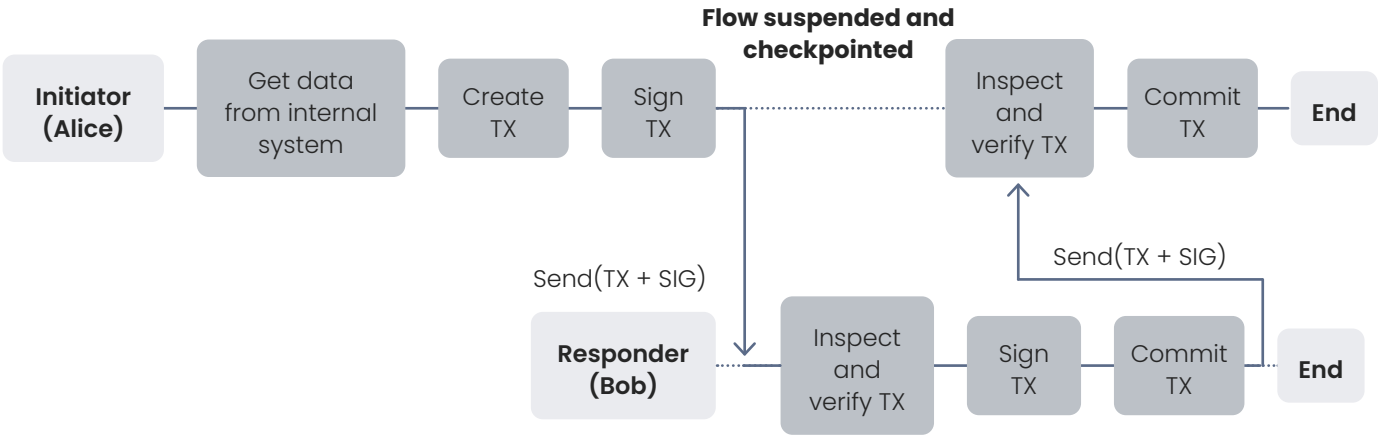
Contracts can be multiple commands, which defines the purpose of the transaction. There could be multiple actions that can be performed on an asset. For example, an update to a vehicle state would be required when it is registered, serviced, insured, etc. Each of these actions would have different business rules, and hence different contract validation logic. To differentiate between different action and run the correct business logic of a transaction, contracts can have multiple commands which allows them to segregate validation rules according to the intent of the transaction.

Flows

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. Once a given business process has been encapsulated in a flow and installed on the node

as part of a CorDapp, the node's owner can instruct the node to start this business process at any time using an RPC call. The flow abstracts all the networking, I/O and concurrency issues away from the node owner.

Transactions are executed in the context of the flows. Each transaction requires certain steps like building the transaction proposal, validating the transaction against the contract, signing the transaction, gathering counterparty signatures, notarizing the transaction, and recording the transaction in all relevant parties involved in the transaction. These steps are encapsulated within a flow and are run when the flow is triggered.



Corda provides a library of flows to handle common tasks, meaning that developers do not have to redefine the logic behind common processes such as:

- Notarizing and recording a transaction
- Gathering signatures from counterparty nodes
- Verifying a chain of transactions

Use-cases

Blockchain has found numerous use-cases in industries ranging from Finance to Supply Chain, Insurance, Healthcare, etc. But while assessing any problem for blockchain solution, it becomes crucial to dive deeper into the specifics of the problem to determine whether Blockchain would be the best solution. At an extremely high level, these are the few questions one could ask while analyzing a problem for blockchain:

- Does the process involve multiple parties to create, share and maintain a transaction record?
- Does the process to share information in a compliant manner involve a lot of manual steps? Does my process for sharing data involve paper?

- Is there a risk that two parties may not see the exact same information?
- Is there a risk of fraud in a given process? Is there a need for long-term recordkeeping and regulatory compliance?
- Is there a need for real-time transfer of assets or payments?

Going further, we will investigate some of the prominent use-cases from the blockchain industry.

Cross border payments (PvP (Payment vs. Payment))

Cross-border payments are transactions where the payee and receiver are based in different countries. The transactions can occur between individuals, companies, or banking institutions that wish to transfer funds across borders and territories. It is a trillion-dollar industry, and the value of cross-border international payment flows is expected to reach $156 trillion in 2022.

Although the world is becoming global and companies are now sourcing and delivering goods and services internationally, the cross-border payment system has not changed significantly. Cross-border systems are still ripe for longstanding problems that existed a decade ago.

The challenge

Cross-border payment is a complex multi-step process involving numerous intermediaries. Research suggests that a majority of the cross-border payment management practices are ineffective both from a cost and time perspective. In the Remittance Prices worldwide report [1] the World Bank states that the global average cost of cross-border payments is as high as 7% approx. Often transferring funds from one country to another could take 2-3 business days and, in most cases, one does not know if or when the money will arrive. Though the cross-border payments are simpler for liquid currencies such as Euro or dollar, for exotic currencies the transactions could take even longer settlement periods and high transaction costs. For example, a transaction from a local bank in Germany to a bank account in Senegal can incur costs of more than 100 Euro, depending on the transaction value, and can take up to 7 days to settle.

The solution

Distributed Ledger technology has the potential to resolve these inefficiencies and provide a secure, faster, and cheap alternative. With Corda, the transactions are instantaneous with no wait for transaction finality. This could support money transfers that are near immediate and final. A DLT based solution would provide these features:

- A global distributed network for payments with banks registered on the network.

- Corda provides the capability to build private but interoperable business networks with transferable assets. These could help with seamless interoperability between multiple consortiums.
- A real-time view of information for everyone on the network.
- Increased transaction performance.

Thus, a DLT based solution will be transparent, secure, cost-effective, and almost immediate with real-time visibility.

Supply-chain

A supply chain is a network between a company, its suppliers, and distributors to produce, distribute and sell a specific product to the final buyer. The network includes different activities, people, entities, and information. The supply chain also represents the steps taken to get the product from its original state to the customers. Thus, supply-chain constitutes a range of planning activities such as demand planning, procurement, product development, marketing, sales, operations, distribution, and customer service. The management of these processes executed to lower costs and boost profitability is called supply chain management (SCM). The objective of supply chain management processes is to help with faster delivery of goods, reduced delays, and better return cycles. All this, in turn, could help with better customer service and satisfaction.

The challenge

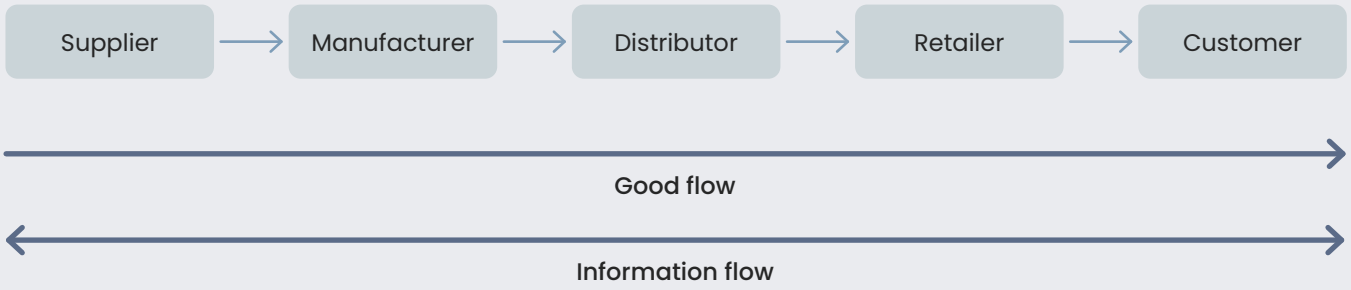
The supply chain process involves multiple participants such as manufacturers, vendors, warehouses, logistics/transportation, retailers, customs, and customers. These participants and the process vary with the type of good, geo-political regulations, and multiple other factors. The supply-chain process constitutes the flow of goods, information, and money. The goods flow includes a flow of an item from the manufacturer to the customer. This happens through various warehouses among distributors, dealers, and retailers. The information flow happens in both directions. The information flow includes documents such as requests for quotation, purchase order, confirmation of purchase order, dispatch details, reports on inventory, invoices, shipment information, etc. The money in turn flows from the customer to the supplier. Overall, the supply chain ecosystem includes multiple parties and entities that all work together to deliver goods to consumers. Information is exchanged between the entities throughout the process. Some of this information should be private to some parties while others should be shared with all entities on the network. The document and verification must be carried out at all stages of the SCM process. It is a manual

process where each entity has its own ledger for goods and products. This leads to lengthy controls and reviews, which increases the expenditure of time and increases costs.

Errors in the supply chain process can lead to huge economic and PR losses. In case of any defects, returns, and recalls it becomes essential to track and trace the goods. With a better supply-chain management process frauds could be detected. Anti-counterfeit goods could be verified easily. This could help companies follow regulations, especially in the food and pharmaceutical industry.

What are the key challenges faced by the current system?

1 **Transparency** 2 **Privacy** 3 **Traceability** 4 **Compliance**



The solution

Digitizing the system with a DLT could contribute to better business processes and workflows. The multiple parties could form part of a same DLT network. Information and documents could be shared in an unambiguous and transparent setting. Disputes could be resolved easily and speedily. The regulators and compliance authorities could become part of the same network. This could help with better compliance checks and approvals.

Central bank digital currency

The challenge

In 1794, the bank of England became the first national bank to regularly issue banknotes as an alternative to coins as a means of payment. And today, two centuries later, all countries around the world use banknotes as payment. With the advancement of technology, money is now going digital. The world is moving towards digital money with payments, with Scandinavian countries leading the

charge. As new the latest reports, the Scandinavian economy is on the verge of going entirely digital, with currently only 10% of their transactions happening in cash. This shift of paradigms is also apparent in the increasing popularity of cryptocurrencies such as Bitcoin, Ethereum, etc. All these cryptocurrencies use DLT as their underlying technology and are decentralized with no involvement of any bank or authority. They have made payments quick and intermediary-free, but they come with major drawbacks and limitations that cannot be overlooked.

Firstly, these currencies don't have any assets backing them up. There is no suitable reserve maintenance to back up the valuations of these cryptocurrencies. They lack the legal and regulatory safeguards that central bank-issued currency has. Adding fuel to the fire, the continued launch of new cryptocurrencies has also raised concerns about the possibility of thefts, frauds, and hacks.

As a result, many central banks across the globe are now working on or contemplating launching their own versions of digital currency. This digital currency will be issued by the central bank directly to the banks or the consumers. These regulated currencies are called central bank digital currencies. They would be acting as a digital version of banknotes and coins, enabling people to hold and make payments in central bank money. They are operated by the respective monetary authorities or central banks. Like the paper-based currency holding a unique serial number, the CBDCs (Central Bank Digital Currency) (Central Bank Digital Currency) will also have unique identifiers and the blockchain platform will itself protect against counterfeiting. Today 85% of central banks are exploring CBDC (Central Bank Digital Currency) and 60% are experimenting [2]. CBDCs could speed up transaction time for individuals and large institutions. They could help grow the ecosystem for multiple other use-cases such as Cross Border Payments, Securities Settlement, improving the RTGS (REAL TIME GROSS SETTLEMENT) systems, Instant Settlements, Remittances, etc.

CBDCs could further be divided into 2 categories:

- **Wholesale CBDC:** Wholesale CBDC refers to a network that is restricted to financial institutions that may hold reserves with the Central bank.
- **Retail CBDC:** General purpose CBDC that will cover a wide range of users such as corporates, merchants, and even the general public.

The solution

A DLT based solution will make processes faster and secure. It will enable p2p payment between financial institutions and banks without compromising the privacy of a transaction and its participants. In the case of cross-border payments, it will reduce

counterparty risks by enabling payment-vs-payment settlement for different currency pairs. R3's Sandbox for Digital Currencies is a learning and development platform for CBDC experimentation used by global financial institutions and regulatory bodies.

Trade Finance

The trade finance ecosystem remains a fragmented ecosystem highly dependent on paper processing and the multiple participants in the transaction lifecycle. These processes burden all the companies involved – importers, exporters, insurers, banks, export credit agencies, and various service providers. With the increasing operational costs and risks, the industry needs solutions and innovations to simplify, manage and digitize trade. Trade finance refers to the financing of international trade flows. As per World Trade Organization, about 80% of world trade relies on trade finance.

What is trade finance and why do we need it?

All of us know about the regular trade processes of lending, borrowing, loans, debts, mortgages, etc. International trade is much complex than the common cash flow of lending and receivable finance.

Let us take a simple scenario of an exporter - Alice and importer – Ben located in USA and Japan respectively, who want to trade with one another. The exporter Alice wants to sell the goods and wants payment in return. The importer Ben wants to purchase these goods. Often these parties don't know each other. Hence, there is a natural trust deficit that exists in this scenario. Alice wants assurance that the payment would be made on completion of delivery. She may also want some part of the payment upfront. She wants to ensure that the order will not get canceled anytime in the future before she starts manufacturing and procuring goods and loading them for shipping. It could result in huge losses, and she would like to mitigate these risks. On the other hand, Ben is worried whether Alice would deliver. He would want to make payment only after ensuring the quality of goods.

Similarly, when the trade takes place across borders there are risks associated with it:

Payment risk
Will the exporter be paid in full and on time?
Will the importer get the goods they wanted?

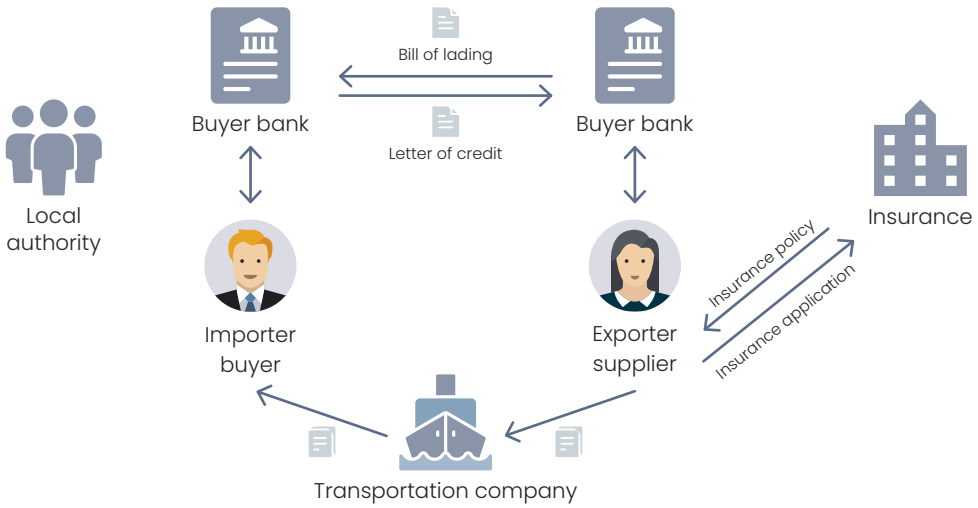
Country risk
A collection of risks associated with doing business with a foreign country, such as exchange rate risk, political risk, and sovereign risk. For example, a company may not like exporting goods to certain countries because of the political situation, a deteriorating economy, the lack of legal structures, etc.

Corporate risk
The risks associated with the company (exporter/ importer): what is their credit rating?
Do they have a history of non-payment?

This is where banks and financial institutions come into the picture. These banks and institutions act as intermediaries inculcating trust in the process for smooth business operation. For the above scenario, the common solution is for the importer's bank to provide a letter of credit to the exporter's bank. The document assures payment from the importer's bank when the exporter presents documents that prove the shipment occurred, for example the bill of lading or the electronic bill of lading (eBL). The letter of credit guarantees that once the issuing bank receives proof that the exporter shipped the goods and the terms of the agreement have been met; it will issue payment to the exporter. Thus, with the letter of credit, the importer's bank assumes the responsibility of paying the exporter.

The importer's bank would need to ensure that the importer was financially viable enough to honor the transaction. Trade finance allows both importers and exporters access such solutions to mitigate the risk associated. Along with mitigating the associated risk, trade finance provides several financial tools that could help bridge the funding gap that may arise due to late shipments, delivery, and payments.

Trade finance diagram



The challenge

The processes are lengthy and inefficient with no automation. There is lots of paperwork and human intervention for reconciliation and verification. All this makes the lifecycle expensive with huge operational costs.

The solution

A DLT based solution will provide a single source of truth for all data relating to agreements, shipments, etc accessible to all authorized people. This easy access to information along with the detailed transaction log would lead to faster verification

and reconciliation. It would also lead to faster tracking, authority checks, and approvals.

Conclusion

These few use-cases would help you understand some of the applications for DLT, but those are just the tip of the iceberg. There are numerous other use-cases that have not been listed due to the restricted scope of this document, some of which could be found here to get more understanding about the possible business solutions. Though one should not see blockchain as a magic bullet, the technology has proven its potential to solve some acute business problems.

Further reading & references

1. remittanceprices.worldbank.org/sites/default/files/rpw_report_december_2016.pdf
2. www.bis.org/about/bisih/topics/cbdc.htm
3. www.forbes.com/sites/forbestechcouncil/2019/03/12/how-blockchain-is-transforming-cross-border-payments/?sh=a0841ac7df2a
4. www.ey.com/en_in/banking-capital-markets/how-new-entrants-are-redefining-cross-border-payments
5. www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp
6. www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/lu-are-central-bank-digital-currencies.pdf
7. Why central banks want to launch digital currencies | CNBC Reports
8. www.investopedia.com/terms/s/supplychain.asp
9. www.investopedia.com/terms/t/tradefinance.asp
10. www.gtreview.com/what-is-trade-finance/

Documentation: docs.corda.net/docs/corda-enterprise/4.8.html

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

Videos: developer.r3.com/videos

Community: community.r3.com

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