What is Corda?

Corda blockchain is best defined as an open-source that solves business problems by providing an interoperable blockchain network. Its key features include strict privacy, efficiency, and direct transactions using smart contract technology.

The smart contracts used in Corda can be written using JVM languages or Java. The dApps within the Corda platform is known as CorDapps. Also, they offer peer-to-peer nodes network with the ability to use Notary infrastructure. The infrastructure is used to validate and sequence transactions without needing to broadcast the transaction details to every peer on the network.

Another important component used by the blockchain includes the Flow framework, which manages the negotiation and communication among participants.

- *Understanding the Corda Ledger*

Corda Ledger is not similar to the ledger system utilized by traditional blockchain technologies. That's why we need to have a clear grasp of how it works and understand it from both its functional point of view and data perspective.

The Corda ledger works like a graph. All the nodes in a graph are connected through each other, either directly or through some other nodes. All nodes can communicate with each other if they want to. The use of the graph means that there is no need to broadcast the transaction globally.

- *Nodes discovery*

So, how do the nodes discover each other? They use a Network map to find each other. You can think of it, similar to a phone book. The Network map contains the metadata to locate each of these services and hence provides a nice way for map discovery.

How Does It Work?

The biggest challenge in a non-global broadcast blockchain network is consensus. So, how do the nodes know about each other and verify that information?

The answer here is shared facts. Each node overlaps any other node in some way or another. The shared facts are stored in the Corda ledger, which can then be used to verify the information. The Corda ledger contains a set of these sets. As there is no central node, these nodes act proxy when there is a need to verify things. To store that information, each node has a vault that contains the fact which cannot be changed. This is how developers implement blockchain.

- *States*

States in the Corda blockchain are immutable. They are used to store shared facts about a transaction, agreement, or contract at a specific point of time.

Sounds technical? Let's try to break it down in simpler words.

- *Shared facts*

Let's take two people using the Corda ledger. Let's name them Alpha and Bravo.

Both of them have a shared fact. The shared fact is an IOU (I Own You). IOU is used when a lender has money due to the loan provider. To make the fact shared, both of them have the same shared information represented in the IOU.

- *Represent Anything*

States can be used to represent anything. This means that it can store any form of information for different corda use cases. As a developer, you can use states to store KYC information, financial instruments, syndicated loans, and so on.
Also, states can be used to store multiple attributes. But there is a limitation for states. The limitation is that once a state is given a type, its type cannot be changed. If you create an IOU state, then it will have to state the IOU state for the rest of its life.

- *Immutable and Evolving*

States are created to be immutable. However, their immutability is concerning time. A state is presented at a given time.

This means that a new state can be created in addition to the original state. It is done when there is a new change made to the state that needs to be stored. The old state is then termed as historical.

For example, if Alpha pays off its debt to Bravo, then a new state will be created, citing the fact that Alpha has cleared the debt. Also, if the state is completed, the IOU will expire. In simple terms, the life cycle of the state, in this case, is as follows.

1. A first state is created to showcase that Alpha is under debt to Bravo. This states also share more information about the IoU, including the date, time, interest rate, the amount lent, and other useful information required for the IoU.
2. Now, when Alpha resolves the debt, a new state is created that updates the new information. The old state is not touched in any way as it is immutable.
3. The new state is now updated in the shared facts among the two users.
4. Now, the old state is termed as historic. There can be multiple historical states in one single transaction. This can lead to creating a sequence of states.
5. A sequence head is created, which refers to the latest state. Also, the latest states are also termed as unconsumed.

What Is Ripple?

Ripple is a blockchain-based digital payment network and protocol that uses its own cryptocurrency, XRP. Ripple's main focus is as a payment settlement asset exchange and remittance system, similar to the SWIFT system for international money and security transfers used by banks and financial intermediaries dealing across currencies.

The token used for the cryptocurrency is premined and uses the ticker symbol XRP. Ripple is the name of the company and the network, and XRP is the cryptocurrency token. The purpose of XRP is to serve as an intermediate mechanism of exchange between two currencies or networks—as a sort of temporary settlement layer denomination. Ripple was first released in 2012 and was co-founded by Chris Larsen and Jed McCaleb.[1][2]

KEY TAKEAWAYS

- Ripple is a blockchain-based digital payment network and protocol with its own cryptocurrency, XRP.
- Rather than use blockchain mining, Ripple uses a consensus mechanism, via a group of bank-owned servers to confirm transactions.
- Ripple transactions use less energy than Bitcoin, are confirmed in seconds, and cost very little, whereas Bitcoin transactions use more energy, take longer to confirm, and include higher transaction costs.
- Ripple (XRP) ranks among the most valuable blockchain-based tokens by market capitalization.
- The Ripple payment system is intended to be used primarily by banks, but individual investors can speculate on the price of XRP.

Understanding Ripple

Ripple operates on an open-source and peer-to-peer decentralized platform that allows for a seamless transfer of money in any form, whether it's dollars, yen, euros, or cryptocurrencies. It is a global payments network and counts major banks and financial services institutions among its customers. XRP is used to facilitate quick conversion between different currencies.[3][2]

Ripple as a Digital Hawala Network

To understand how the system works, consider a money transfer structure where the two parties on either end of the transaction use their preferred intermediaries to receive the money. In effect, Ripple functions as a digital hawala service. Hawala is an informal method of transferring money, usually across borders, without any physical money actually moving.[4]

For example, imagine Lawrence needs to send $100 to River, who lives in a different city. Lawrence sends the funds to a local agent, Kate, and provides a secret password that River must correctly answer to receive the funds in their city. Kate alerts River's agent, Asuka, of the transaction details—recipient, funds to be reimbursed, and password. If River gives Asuka the right password, Asuka gives them $100.

However, the money comes from Asuka's account, which means that Kate owes Asuka $100 (which will be settled at a later date). Asuka can either record a journal of all Kate's debt, which Kate would pay on an agreed day, or make countertransactions that would balance the

debt. This multi-step transaction requires a network of trust, which Ripple bypasses using a blockchain network.

Any person or business can register and open a gateway, which authorizes the registrant to act as the intermediary for exchanging currencies, maintaining liquidity, and transferring payments on the network.5

Ripple's Digital Currency XRP

Ripple's digital currency, XRP, acts as a bridge currency to other currencies. It does not discriminate between any fiat/cryptocurrency, which makes it easy for any currency to be exchanged for another. Each currency on the ecosystem has its own gateway—for example, CADBluzelle, BTCbitstamp, and USDsnapswap. If River wanted bitcoins as payment for the services rendered to Lawrence, Lawrence does not necessarily have to be in possession of any bitcoins. He can send the payment to his gateway in Canadian dollars (CAD), and River can receive bitcoins from his gateway. One gateway is not needed to initiate a complete transaction; multiple gateways can be used, forming a chain of trust rippling across the users.

Holding balances with a gateway exposes the user to counterparty risk, which is also present in the traditional banking system. If the gateway does not honor its liability, the user could lose the value of money held at that gateway. Users who don't trust a gateway can, therefore, transact with a trusted gateway that deals with the "untrusted" gateway. This way, the IOU will be transacted through a trusted or creditworthy-certified gateway.

How Ripple Works

The Ripple network does not run with a proof-of-work (PoW) system like Bitcoin or a proof-of-stake (PoS) system like Ethereum. Instead, transactions rely on a consensus protocol to validate account balances and transactions on the system. The consensus works to improve the integrity of the system by preventing double-spending.

A Ripple user that initiates a transaction with multiple gateways but attempts to send the same $100 to the gateway systems will have all but the first transaction deleted. Individual distributed nodes decide by consensus which transaction was made first. The confirmations are instant and take roughly five seconds. Because no central authority decides who can set up a node and confirm transactions, the Ripple platform is described as decentralized.

The XRP Ledger keeps track of all IOUs in a given currency for any user or gateway. IOU credits and transaction flows between wallets are publicly available on the XRP ledger. But even though financial transaction history is publicly recorded and made available on a blockchain, the data is not linked to the ID or account of any individual or business. However, the public record of all dealings (i.e., the blockchain) makes the information susceptible to de-anonymization measures.6

The Ripple payment system is mainly intended to be used by banks, although individual investors may speculate on the price of XRP.

Special Considerations

Ripple improves on some of the drawbacks attributed to traditional banks. Transactions are settled within seconds on the Ripple network (even though the platform handles millions of transactions frequently).

This is unlike banks, which could take days or weeks to complete a wire transfer. The fee to conduct transactions on Ripple is also minimal, with the minimum transaction cost required for a standard transaction set at $0.0002 XRP, compared with the hefty fees charged by banks for conducting cross-border payments.[7][2]

Is Ripple Better Than Bitcoin?

Ripple transactions use less energy than Bitcoin, are confirmed in seconds, and cost very little, whereas Bitcoin transactions use more energy, take longer to confirm, and include higher transaction costs.[8][2]

How Does Ripple's Network Function?

Ripple network transactions rely on a consensus protocol to validate account balances and transactions on the system. It does not run with a PoW system like Bitcoin or a PoS system such as Ethereum. Ripple's consensus aims to improve the integrity of the system by preventing double-spending.

How Is Ripple Different from XRP?

Ripple is a global payments network with major banks and financial services providers as its customers. XRP is an open source cryptocurrency developed by Ripple that is used in Ripple products to facilitate quick conversion between different currencies.

The Bottom Line

Ripple is a decentralized blockchain designed to provide payment services that are faster than existing solutions for institutions globally using its native cryptocurrency, XRP.

What is Quorum Blockchain?

For enterprise applications, Quorum Blockchain is a permissioned blockchain technology that offers fast transaction throughput, privacy, and security. Given that it is built upon Ethereum, many of its capabilities, including smart contracts and decentralized applications, are passed down to it. Quorum, however, has certain qualities of its own that make it perfect for business use cases.

Quorum blockchain is a permissioned blockchain platform with the following key features.

- **Privacy and Security –** To provide transaction privacy, Quorum makes use of Constellation, a private transaction manager. It is perfect for confidential enterprise applications because only those parties involved in a transaction may see the specifics.
- **High Transaction Throughput –** The QuorumChain consensus algorithm allows Quorum to process thousands of transactions per second.
- **Smart Contracts and Decentralized Applications –** Quorum is appropriate for a variety of use cases since it facilitates the creation of smart contracts and decentralized apps.
- **Built on Ethereum –** Many of Ethereum's characteristics, such as smart contracts and decentralized applications, are carried over to Quorum, but it also has certain special powers of its own.

Quorum blockchain is designed specifically for enterprise use cases that require privacy, security, and high transaction throughput. By leveraging its unique features, businesses can streamline their operations, reduce costs, and increase efficiency.

Quorum Blockchain Development

Quorum Blockchain development has evolved since its inception in 2016. Conceived by J.P. Morgan, Quorum was later acquired by ConsenSys, a leading Ethereum software company, in 2020. Today, it continues to be actively maintained and improved, with a vibrant community of developers contributing to its success.

Quorum Blockchain Examples

Quorum Blockchain has been adopted by numerous organizations across various industries, including finance, supply chain, and healthcare. Some noteworthy examples include

- **J.P. Morgan's Interbank Information Network (IIN) –** A global, peer-to-peer network for sharing information between banks, powered by Quorum.
- **Luxembourg Stock Exchange –** Utilizing Quorum to automate the issuance and management of securities.
- **Kadena –** A healthcare platform that leverages Quorum to streamline medical supply chain processes.

Key Features of Quorum

Quorum offers several features that cater specifically to the needs of enterprises, such as

Enhanced Performance: Quorum exhibits superior speed compared to Bitcoin and Ethereum, processing over 150 transactions per second. This efficiency stems from its utilization of a simplified consensus mechanism. By default, Quorum employs the RAFT consensus for fault tolerance and the IBFT consensus for Byzantine fault tolerance, both of which outperform Ethereum's proof-of-work consensus.

Permission Management: Quorum restricts participation to a predetermined group of nodes that must be authorized to join the blockchain network. It operates exclusively among participants who have been pre-approved by a designated authority, thereby ensuring controlled access rather than an open network.

Elimination of Transaction Pricing: Quorum effectively eradicates the notion of transaction costs by eliminating the necessity of cryptocurrency-based expenditures, such as gas. Although Quorum's foundational code was originally derived from Ethereum, it has been engineered to render gas utilization in transactions non-existent.

Enhanced Privacy: Quorum offers a comprehensive approach to transaction privacy by facilitating both on-chain public and private transactions. Open transactions function similarly to Ethereum, whereas private transactions remain concealed from public visibility.

Quorum employs Constellation technology to encrypt specific messages within a designated enclave and retains information about past transactions.

Asset Management: Quorum enables entities to autonomously create, manage, and distribute digital assets without the need for third-party intermediaries, thereby bestowing asset owners with enhanced autonomy to dictate the management of their assets.

Open Source: Quorum operates as an open-source platform, with a thriving community of over 300 contributors actively engaged in its ongoing development and enhancement.

Quorum Architecture

Quorum's architecture is built upon the Ethereum blockchain, inheriting many of its features while adding enterprise-specific enhancements. The key components of Quorum's architecture include:

- **Quorum Node**
  Quorum node is the fundamental building block of the Quorum network, responsible for processing transactions, maintaining the ledger, and participating in consensus.
- **Quorum Chain**
  Quorum chain is the underlying data structure that stores transactions and ensures their immutability.
- **Consensus Mechanisms**
  Quorum supports multiple consensus mechanisms, such as Raft and Istanbul BFT, allowing organizations to choose the one that best suits their needs.
- **Smart Contracts**
  Like Ethereum, Quorum enables developers to write and deploy smart contracts to automate business processes and create decentralized applications (DApps).
- **Quorum Network Manager**
  The Quorum Network Manager (QNM) is a component that manages access to the network, ensuring that only authorized nodes can participate.

What Is Decentralized Finance (DeFi)?

Decentralized finance (DeFi) is an emerging financial technology based on secure distributed ledgers similar to those used by cryptocurrencies.

In the U.S., the Federal Reserve and Securities and Exchange Commission (SEC) define the rules for centralized financial institutions like banks and brokerages, which consumers rely on to access capital and financial services directly. DeFi challenges this centralized financial system by empowering individuals with peer-to-peer transactions.

KEY TAKEAWAYS

- Decentralized finance, or DeFi, uses emerging technology to remove third parties and centralized institutions from financial transactions.
- The components of DeFi are cryptocurrencies, blockchain technology, and software that allow people to transact financially with each other.
- DeFi is still in its infancy, subject to hacks and thefts because of sloppy programming and a lack of security testing before applications are launched.

How Decentralized Finance (DeFi) Works

Through peer-to-peer financial networks, DeFi uses security protocols, connectivity, software, and hardware advancements. This system eliminates intermediaries like banks and other financial service companies. These companies charge businesses and customers for using their services, which are necessary in the current system because it's the only way to make it work. DeFi uses blockchain technology as a way to reduce the need for these intermediaries.