XRP Ledger

Earlier known as “Ripple”

XRP Ledger

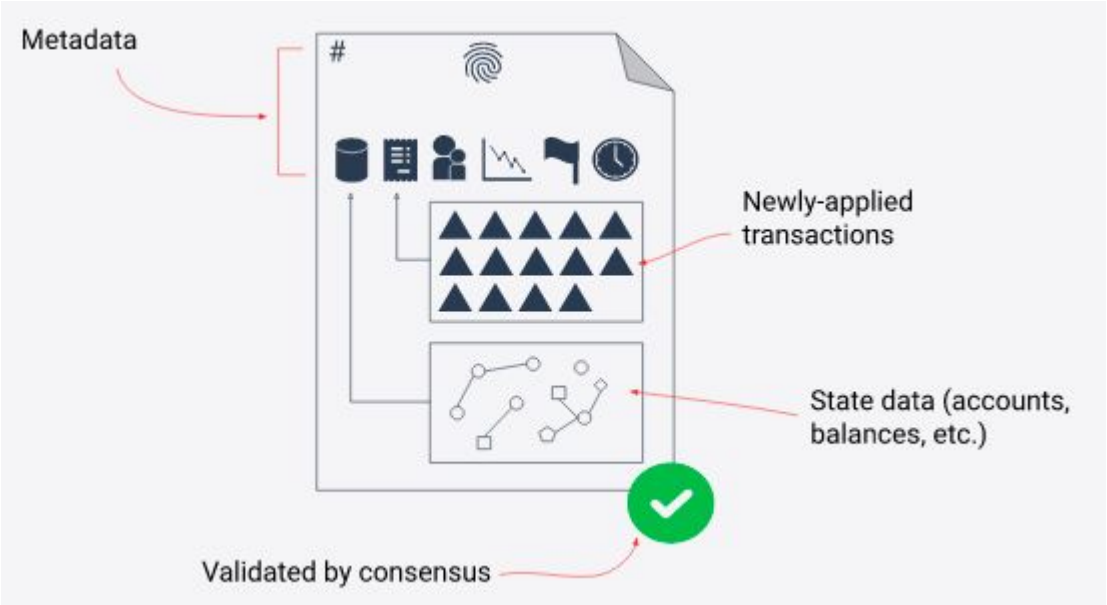
- developed by David Schwartz, Jed McCaleb, and Arthur Britto, 2011
- native cryptocurrency used is **XRP**
- first blockchain to support the **tokenization of various assets.**

Key benefits

- Faster transactions
  - roughly 3-5 seconds at a global scale
- Low cost transaction
  - less than one cent, starting at just 0.0001 XRP (10 drops)
- Sustainable
  - No mining! No need for energy-hungry servers that use up a lot of electricity.
  - Quorum-based consensus protocol

XRP Ledger

XRP Ledger processes transactions in blocks called "ledger versions", or "ledgers" for short



XRP Ledger

How is Ripple Different From Other Cryptocurrencies?

- Lack of incentive for validators
  - No gain in being a validator
- Ripply supply
  - XRP is neither mined nor minted, but rather 100 billion XRP was pre-mined at the launch
  - 80 million of which is released through **Escrow** account
- Speed and transaction costs
  - 3-5 seconds
- Bridge currency
  - allows users to denominate their transactions with any currency
  - including fiat currencies, digital currencies, and other forms of value like gold
- Tokens as IOUs (I owe you)

XRP Ledger

New concepts

- Unique Node List (UNL)
- Payment channels (for micro-payments)
- Escrows
  - hold funds in a secure account until certain conditions are met or a specified time period has elapsed.
- Checks
- Multi-signature accounts
- IOUs and NFTs (with a smart contract)
- Dex (decentralized Exchange)
  - Auto-bridging and path-finding through order books
- Stablecoins

XRP Ledger Consensus Protocol

Trust-Based Validation

- **Validators**

  - servers specifically configured to participate actively in consensus
  - responsible for validating the transactions
  - expected to behave honestly most of the time according to the protocol.

- **Unique Node List, or UNL**
  - List of chosen validators maintained independently by each server
  - a server accepts transactions only from the validators in its UNL
  - Can be modified via pseudo-transactions

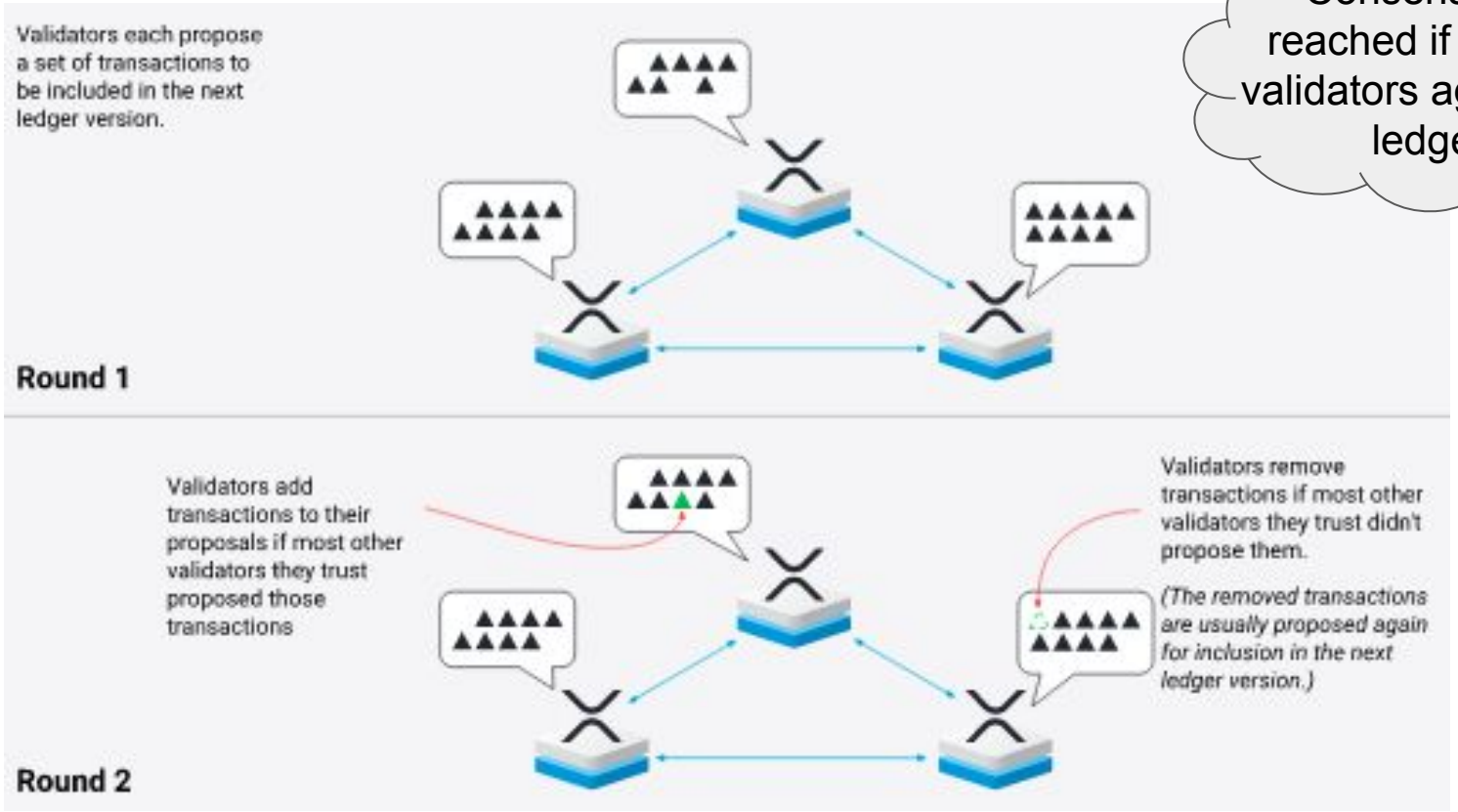
How XRPL works?

With each transaction on the XRPL, these steps happen within seconds:

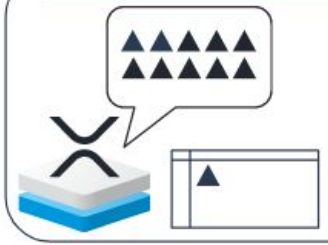
1. Transactions on the XRPL are sent to individual validators.
2. The validators
    a. check if the transactions follow the rules of the ledger.
    b. Proposes next ledger by sharing it with others in their UNL, comparing it with those of other validators they trust, checking each new transaction for validity.
3. If there's an agreement, the transaction is confirmed and added to the ledger.
4. If they don't agree,
    a. validators modify their proposals to more closely match the other validators they trust, repeating the process in several rounds until they reach a consensus.

XRP Ledger Consensus Protocol

Consensus is reached if 80% of validators agree to a ledger



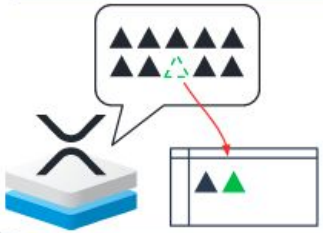
Consensus Round 1



Each validator proposes a set of transactions to be included in the next ledger version.

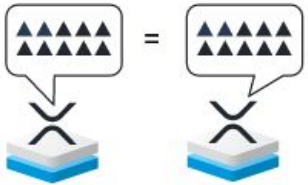
Each also keeps a queue of candidate transactions not currently proposed.

Consensus Round 2



If a validator removes a transaction from its proposal in later rounds, it adds that transaction to its queue.

Consensus Round N

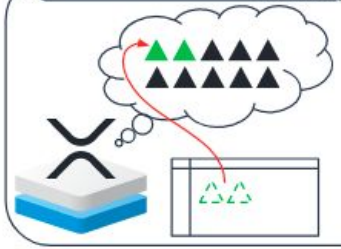


The consensus process continues until enough servers agree on a transaction set.

Validation

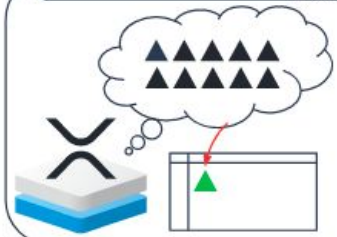
Servers confirm that they built the same resulting ledger and declare it validated.

Building the Next Proposal



Each validator prepares its proposal for the next ledger version, starting with queued transactions.

Adding to the Queue



If the next proposed ledger version is already full, incoming transactions are queued for later.

(Next ledger version)

Consensus Protections Against Attacks and Failure Modes

Individual Validators Misbehaving

- As long as 80% validators remain honest, this is not a problem

Software Vulnerabilities

- open-source code base, thorough and robust code review process ,
- Digital signatures from Ripple employees on all releases and official software packages,
- Regularly-commissioned professional reviews for security vulnerabilities and insecurities.
- bug-bounty program rewards security researchers who responsibly disclose vulnerabilities.

Sybil Attacks

- servers only listen to the validators they are configured to trust, either through a validator list or explicit configuration.

XRPL Transactions

- A Transaction is the only way to modify the XRP Ledger.
- Finalised only if signed, submitted, and accepted into a validated ledger version following the consensus process.
- Pseudo-transactions (for amendment, set fee or modifying UNL), which aren't signed or submitted, but still must be accepted by consensus.
- Failed transaction also included in ledgers because they modify balances of XRP to pay for the anti-spam transaction cost.
- Other than payment, transactions in the XRP Ledger are also used to
  - rotate cryptographic keys,
  - manage other settings, and
  - trade in the XRP Ledger's decentralized exchange.

XRPL Transactions

Transaction cost/fees

- each transaction automatically burns a small amount of XRP, which starts at 0.00001 XRP (10 drops).
- Debited from the sender’s account but not paid to validator
- Designed to increase in parallel with the load on the network, making it expensive to deliberately or inadvertently overload the network.

XRPL Payment Types

- Direct XRP Payments
  - Peer-to-peer cryptocurrency XRP payments
- Cross-Currency Payments
  - atomically deliver a different currency than they send by converting through paths and order books.
- Checks
  - deferred payments that can be canceled or cashed by the intended recipients.
- Escrow
  - set aside XRP and deliver it later when certain conditions are met.
- Partial Payments
  - subtract fees from the amount sent, delivering a flexible amount.
- Payment Channels
  - enable fast, asynchronous XRP payments that can be divided into very small increments and settled later

Accounts on the XRP Ledger

represents a holder of XRP and a sender of transactions.

core elements of an account are:

- An identifying address, such as rf1BiGeXwwQoi8Z2ueFYTEXSwuJYfV2Jpn.
- An XRP balance. Some of this XRP is set aside for the Reserve.
- A sequence number, which helps make sure any transactions this account sends are applied in the correct order and only once each.
- A history of transactions that affected this account and its balances.
- One or more ways to authorize transactions eg: Multi-signed transactions

Accounts on the XRP Ledger

- All accounts have a **public address** and a **private key.**
- Accounts can hold **multiple currencies** and asset types at once
- A small XRP refundable deposit (“**base reserve**”) is required to open an account on the XRPL, to prevent spamming of network
- An **exchange wallet** can manage wallets for multiple people using a single address with a destination tag to specify the user’s address.
- Single account can be managed by multiple users through **key rotation**

Accounts on the XRP Ledger

Typical way to **create an account** in the XRP Ledger is as follows:

- **Generate a key pair** from a strong source of randomness and calculate the address of that key pair.
- Have someone who already has an account in the XRP Ledger **send XRP** (not lesser than reserve requirement) **to the address** you generated.

Accounts on the XRP Ledger

Account has **reserve requirement** consisting of two parts:

Base Reserve

minimum amount of XRP that is required for each address in the ledger.

Owner Reserve

Amount for each object that the address owns in the ledger.

The cost per item is also called the incremental reserve.

What do u think happens if the reserve goes below the minimum requirement?

Stablecoins

- **Token that represent real-world assets**, like the US dollar, piece of art, or a physical commodity.
- **exchange rate** between the token and the asset it represents should be "**stable**" at ideally 1:1

Stablecoin issuers (formerly called "**gateways**")

- link tokens in the XRP Ledger to **real-world assets**
- already has a system to accept deposits and withdrawals from some outside payment source.
- waits for deposits to clear before crediting them in system of records
- always keeps enough funds on-hand to pay withdrawals on demand

XRPL’s decentralized exchange (DEX)

first blockchain to feature a built-in decentralized exchange (DEX).

The XRPL DEX:

- Allows to trade XRP or tokens without having a centralized exchange.
- is trustless—need not worry about losing assets to hacks or thefts
- is also non-custodial, can retain full control of your assets at all times.

XRPL’s decentralized exchange (DEX)

Auto bridging uses XRP as an intermediary asset to find the best exchange rate.

Pathfinding uses a series of assets to “hop” from one currency or form of value to another, finding the best path with the best route to go from one form of value to the other.

For example, if a seller wanted to trade their XRP for tokenized gold, pathfinding may find that the best solution is to first trade XRP for USD, and then trade that USD for tokenized gold.

XRPL’s decentralized exchange (DEX)

Just like with a centralized exchange, the XRP DEX uses a ‘bid’ and ‘ask’ system.

Bid: A buyer can specify a price they want to buy at or below

Ask: A seller can specify a price they want to sell at or above

Example: Let’s assume the current price of XRP is $0.50. If a seller wants to sell their XRP for $0.60, they would place an ask order at $0.60 on the DEX. If a buyer wanted to buy XRP for $0.40, they would place a bid order at $0.40 on the DEX.

All bids and asks for each asset are tracked in an order book on the ledger for transparency.

XRP Ledger

How Does Ripple Make Money?

- sells XRP from its escrow accounts
- Burned transaction fees goes to ripple
- profits from investments
- Interest on loans

Acknowledgement

All contents of this presentation in taken from the following sites:
https://corporatefinanceinstitute.com/resources/cryptocurrency/ripple/
https://xrpl.org/docs.html