

Alibaba Cloud

LedgerDB Product Introduction

Document Version: 20200908

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions









Style	Description	Example
 Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings> Network> Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.What is LedgerDB?	05
2.Scenario	07
3.Limits	08

1.What is LedgerDB?

The trusted ledger database (LedgerDB) provides blockchain database services. The service combines the high performance and low latency of a centralized system with the non-tampering and non-repudiation of data in the blockchain. It avoids the high cost and threshold of access to the blockchain and is suitable for various data recordation and data tracing scenarios.

Features

Highly reliability

LedgerDB ensures that all data written into LedgerDB is highly reliable (tamper-resistant and non-repudiation). At the same time, any non-read operation of the ledger is recorded, thus realizing the high reliability of the data throughout the life cycle of the entire Ledger data. As the service provider of LedgerDB, LedgerDB did not have the ability and willingness to modify the data, thus achieving the "self-certification" of the service provider.

- The storage layer uses the block-chain storage structure ensured by digital cryptography and the improved data structure of the Merkel transaction accumulator to ensure the tamper resistance of all data stored in the ledger.
- Application layer: adopts the multi-party signature mechanism, which ensures that once data is stored, it cannot be tampered with or verified by any participant.
- Public network layer: introduces a trusted third-party Time Service Center to stamp data with a trusted timestamp, ensuring data credibility in the time dimension.

System High Performance

Based on the core technology independently developed by the universal audited ledger team, data operations on a single ledger and single client can reach 300,000 TPS, with a response delay of milliseconds.

Reduced Storage Costs

In data storage or data tracking scenarios, LedgerDB has lower storage costs than the consortium blockchain solution in scenarios. In the consortium chain, a minimum of four nodes are required. The nodes are stored on cloud disks, and each node stores three copies of data. However, LedgerDB is a centralized service and only needs one node to store three data copies.

Low access cost

LedgerDB provides common database interfaces to allow technical engineers to access it without learning a new contract development language.

Multi-party collaboration

Under the premise of ensuring the characteristics of other products, LedgerDB supports the simultaneous use of the same ledger database by multiple participants, better to meet the business scenarios requiring multi-party collaboration.

Quick data verification

A new chain-like block storage architecture is used to verify the credibility of Ledger data in milliseconds.

Natively traceable data

It provides users with a customizable "data clue" function, which can be used to associate data. Combined with the "high reliability of data" feature of LedgerDB, the data associated with the data clue directly has tamper-resistant data traceability and traceability capabilities.

Regulatory friendliness

Working with member permission management, the regulatory authority and the regulated authority can use the same LedgerDB to meet the requirements of multiple parties.

2.Scenario

As a basic database system, LedgerDB can be used to store business data and enhance the credibility of business data in a variety of scenarios, such as finance, government, medical, IoT, digital copyright, agricultural product traceability, and enterprise credit investigation.

Alternatively, Apsaradb for Oceanbase can be used with existing database products to store system operation logs in a tamper-resistant manner.

3.Limits

During the public beta, the LedgerDB has the following resource restrictions:

Ledger capacity limit	20G
The number of ledgers that can be created for each account	10
The number of ledgers that an account can join	100
Number of members of one ledger	10
TPS	10000
Number of association clues for a single record	32
Single record size	4M
Length of a single clue	128B