Blockchain as a Service

Product Introduction

MORE THAN JUST CLOUD | Alibaba Cloud

Product Introduction

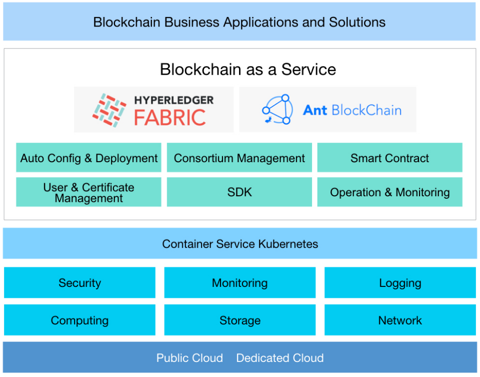
What is BaaS

Alibaba Cloud BaaS (Blockchain as a Service) is an enterprise-level PaaS (Platform as a Service) based on leading blockchain technologies. This service helps you build a stable, secure blockchain environment, and manage the deployment, operation, maintenance, and development of blockchains easily. Alibaba Cloud BaaS enables you to focus on business innovation.

Blockchain establishes a peer-to-peer network where each participant in the network has access to a shared ledger. Transactions and history records cannot be removed or altered. The smart contract and consensus algorithms enable transactions between multiple participants and confirm the transactions and ledger records. For more information about the consensus algorithms and smart contracts, see Hyperledger documentation.

Why blockchain on Alibaba Cloud?

- Alibaba Cloud BaaS is built on Alibaba Cloud Container Service for Kubernetes clusters. It leverages the capabilities of Alibaba Cloud in databases, security, maintenance, and computing. Alibaba Cloud BaaS provisions blockchain services based on multiple architectures, such as public cloud deployments and private cloud deployments.



-Alibaba Cloud BaaS helps users quickly create and deploy a production-level blockchain environment, and provides graphical interfaces for blockchain management and operation. Enterprises and businesses can be dynamically added to the blockchain network. This service simplifies development and reduces the development time with pre-configured networks and infrastructure.

- The consortium blockchain network is built on the Alibaba Cloud BaaS. This network relies on the multi-tenant isolation of cloud computing, including the isolation of computing, storage, and network resources. Business participants are independent and can manage their own resources separately.
- This service provides a cross-regional network for participants in different regions. For example, as shown in the following figure, operators and participants in a consortium blockchain network can be deployed in three different cities.

Beijing
Consortium Operater Organization
Shanghai
Business Participant Organization
Shenzhen
Business Participant Organization

-Alibaba Cloud provides a wide range of methods for you to integrate the blockchain service into your applications. You can create resources on demand and scale up the deployment easily. Additionally, this service provides advanced protection for data security and privacy. You can select the services that best suit your business needs at the optimal costs.

For more information, see Product benefits.

Product editions

The product editions include Basic Edition, Enterprise Edition and Enterprise Security Edition. For a detailed description and comparison of these three product editions, see Product editions.

How to use Alibaba Cloud blockchain service

1. Create a blockchain network

You can create a blockchain network in quick mode or standard mode.

Quick mode: You only need to specify the required information, and Alibaba Cloud BaaS will automatically perform operations to create a complete blockchain network. These operations include creating a consortium, creating organizations, and inviting groups to join a consortium or a channel. For more information, see Quick start with blockchain.

Standard mode: You can manually create an organization, create and join a consortium, and create a channel. For more information, see Use blockchain services.

2. Deploy chaincodes

This step includes uploading, installing, and instantiating the chaincode. For more information, see Deploy chaincodes.

3. Access the blockchain network

This step includes Create users and Access blockchain networks through the SDK.

Advantages

Openness and sharing

- Alibaba Cloud BaaS supports blockchain applications and data under the Hyperledger Fabric framework. Development results are shared to an open source blockchain community.
- Alibaba Cloud will integrate developed blockchain systems to build an open, capable, and standardized blockchain ecosystem for users.

High security

- Based on the on-chip encryption technology of the ECS Bare Metal Instance, this service provides high-level security protection for private keys.
- Supports encryption and decryption based on China’s recommended cryptographic algorithms.
- Establishes a consortium blockchain management system targeting multiple enterprises to facilitate collaboration among enterprises.
- Provides multi-dimensional network isolation, network access control and attack protection for enterprises.
- Each enterprise has an independent CA service to suit their business needs.
- Provides built-in risk control and operation auditing to avoid a “fat-finger error”.
- The Alibaba Financial Cloud based on Alibaba Cloud complies with Grade IV Protection of

Information Security, providing a secure environment for the deployment of your blockchain service.

- Alibaba Cloud provides over 17 security products, 9 security solutions, and 14 security services, to establish a comprehensive security protection system for upper-layer business applications.

High availability

- Provides end-to-end and highly available services, covering blockchain nodes, service administration, and container clusters, to ensure business continuity.
- The bottom-layer storage of the blockchain ledger is highly reliable (99.999999999%) and can scale up quickly without interruption.

Ease-of-use

- Helps you quickly build an enterprise-level blockchain network.
- Alibaba Cloud BaaS provides rich management and operation functions through a graphical interface. This user-friendly service allows all levels of users to get started quickly. You can easily configure, deploy, manage, and monitor multiple blockchain networks owned by an enterprise.
- This service allows you to save bottom-layer infrastructure and daily operating and maintenance costs. This allows enterprises to focus on business application innovation.

High performance

Alibaba Cloud BaaS is based on high-performance cloud servers, including ECS Bare Metal Instance, high-bandwidth network, and high-concurrency and high-throughput storage. This service can maximize the performance potential of blockchains.

Global deployment

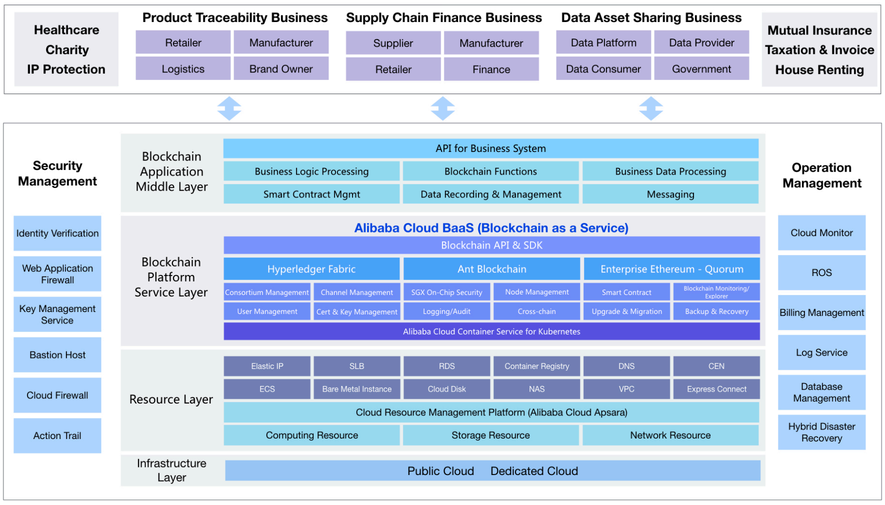
- With data centers around the world, Alibaba Cloud helps you deploy business systems worldwide.
- Based on proven overseas compliance processes and practices of Alibaba Cloud, this service helps you build a secure, compliant, and operational business system.

Architecture

Alibaba Cloud BaaS is built on top of Kubernetes, supports mainstream blockchain technologies, and integrates with the comprehensive services of Alibaba Cloud. BaaS allows users to establish cross-enterprise, cross-region business cooperation and transaction network, and to implement blockchain business scenarios at speed.

Product architecture

- Infrastructure layer: Currently BaaS supports public cloud and private cloud offerings of Alibaba Cloud. And BaaS will support hybrid cloud deployment in near future.
- Cloud resource layer: Provides basic cloud resources for blockchain services and upper-layer applications, including ECS, VPC, NAS, and SLB.
- Platform services layer: Built on Alibaba Cloud Container Service Kubernetes clusters, the blockchain platform supports multiple basic BaaS services. These services include resource creation, resource management, resource operation, and security management. The blockchain engines currently support Hyperledger Fabric 1.4 LTS
- Mid-layer application: This is a reference architecture that is used to connect BaaS with business applications. It is usually implemented in form of blockchain business solution or blockchain middleware.
- The overall architecture also includes multiple services that may be applicable to BaaS, such as security management and operation management.



Scenarios

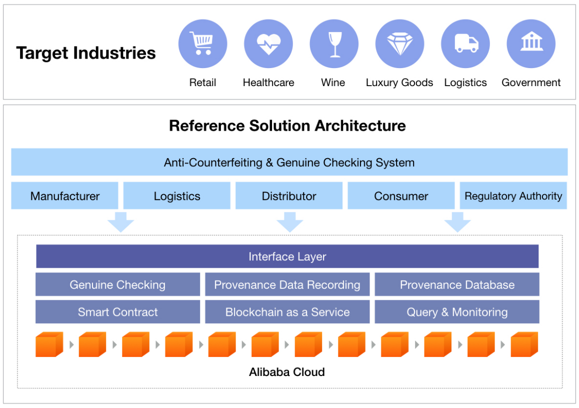
Scenarios

Alibaba Cloud BaaS can be applied to multiple business scenarios, such as product traceability, data asset transactions, supply chain financing, digital content ownership, charity, letters of credit, asset securitization, asset custody, energy and chemical trading, real estate transactions and leasing, and digital identity. The following two scenarios are taken as examples:

Scenario one: product traceability

In conventional retail scenarios, consumer and supply chain information is not traceable. When a product quality or safety issue occurs, it is difficult to trace and recall the product, or locate the responsible party. At the same time, the supply chain information is at risk of counterfeiting and tampering.

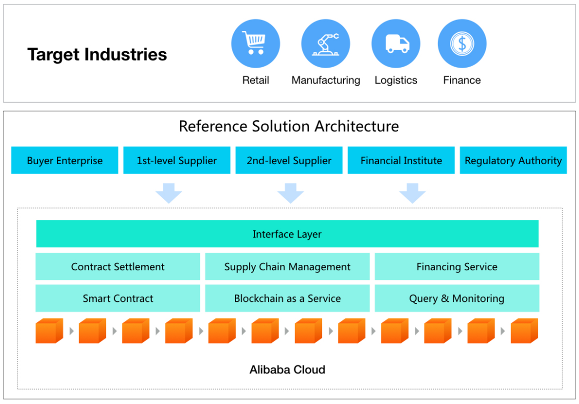
Alibaba Cloud BaaS provides a tamper-resistant shared transaction history. This service supports querying and auditing by consumers. At the same time, the blockchain ensures that the source information is confirmed by all participants and the information cannot be tampered with. The entire transaction history on the blockchain can be audited to meet policy and regulatory requirements. The blockchain can be combined with anti-counterfeiting and digital technologies to provide a complete set of traceability solutions for multiple commodities.



Scenario two: supply chain financing

In conventional transactions, the credit of enterprises cannot be shared securely among key enterprises and suppliers up and down the supply chain. As a result, it is very difficult and inefficient for small and medium-sized enterprises (SMEs) to secure funding. Supply chain information cannot be shared securely. This causes funding inefficiencies. For example, poor instrument negotiation causes long settlement periods.

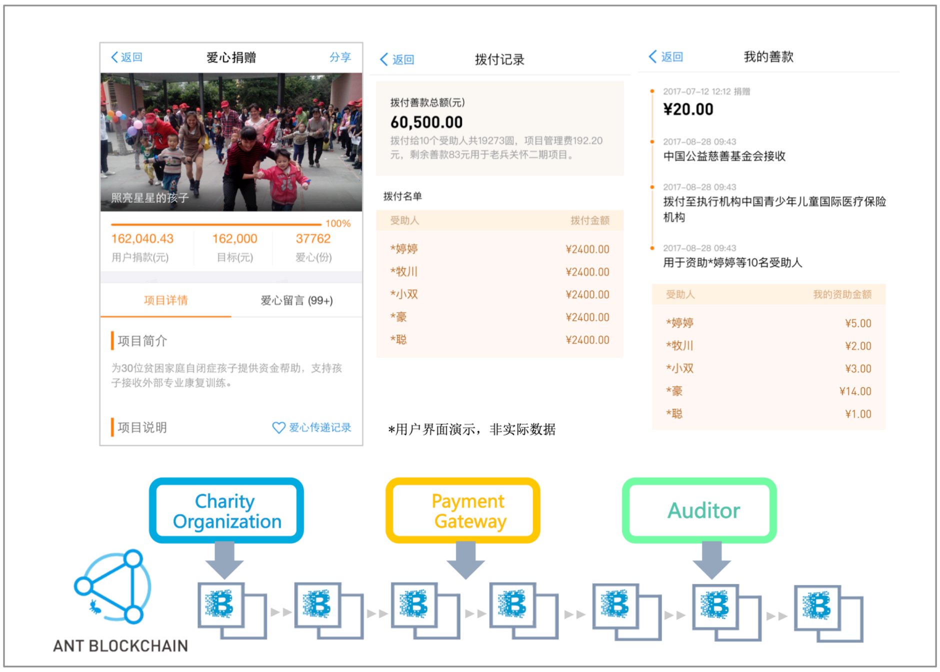
In Alibaba Cloud BaaS, information of the key enterprises, such as receivables and payables, can be shared securely among suppliers, dealers, and financial institutions. The blockchain service can protect private data while sharing the transaction data among enterprises. In addition, the smart contract supports automatic fund clearing and the circulation of corporate bonds, to improve business operations and the efficiency of capital flow.



Scenario three: charity

From donor to beneficiary, end-to-end traceability of charity projects. With transparent and trusted ledger and timely disclosure, the blockchain service enhances mutual trust between donators and public interest organizations, and improves the efficiency of charitable acitivities.

Running live for over 1 year, with 38 charity organizations and 355 charity projects (data at the end of July, 2017).



162,040.43	162,000	37762
用户捐款(元)	目标(元)	爱心(份)

项目简介

为30位贫困家庭自闭症孩子提供资金帮助，支持孩子接收外部专业康复训练。

项目说明

拨付善款总额(元)

60,500.00

拨付给10个受助人共19273圆，项目管理费192.20元，剩余善款83元用于老兵关怀二期项目。

拨付名单

受助人	拨付金额
*婷婷	¥2400.00
*牧川	¥2400.00
*小双	¥2400.00
*豪	¥2400.00
*聪	¥2400.00

*用户界面演示，非实际数据

2017-07-12 12:12 捐赠
¥20.00

2017-08-28 09:43
中国公益慈善基金会接收

2017-08-28 09:43
拨付至执行机构中国青少年儿童国际医疗保险机构

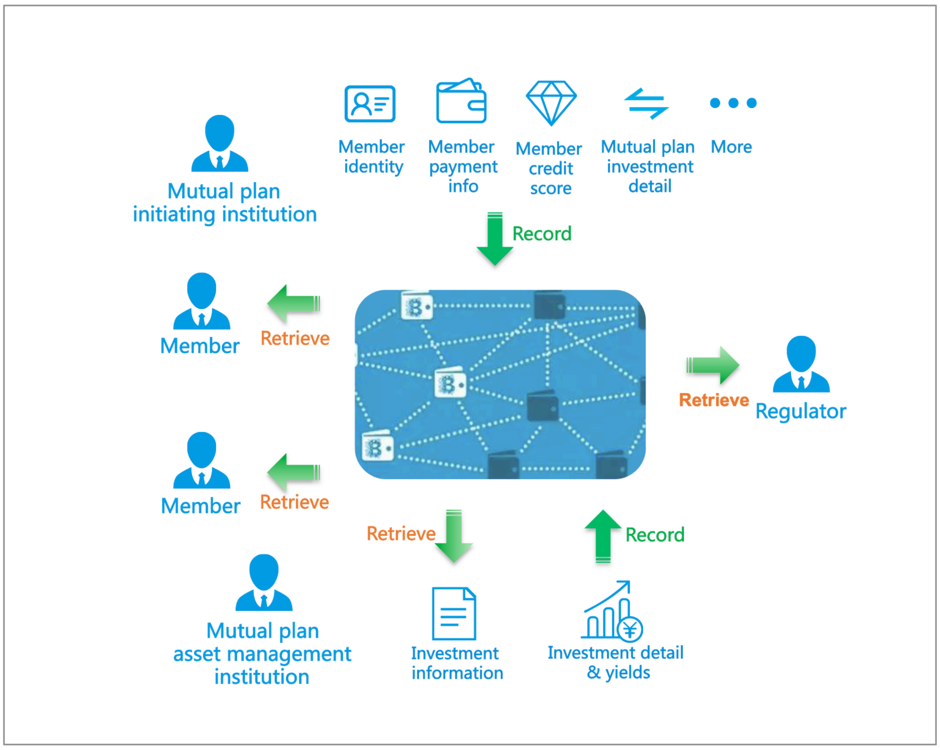
2017-08-28 09:43
用于资助*婷婷等10名受助人

受助人	我的资助金额
*婷婷	¥5.00
*牧川	¥2.00
*小双	¥3.00
*豪	¥14.00
*聪	¥1.00

Scenario four: mutual insurance

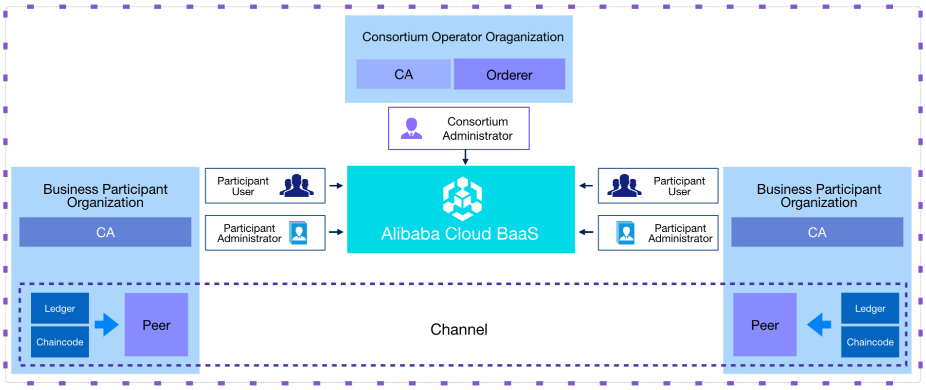
This model is based on a certain group of people forming an insurance risk pool and support each other without a trust center. In this case, it is especially important that how to make sure the usage of insurance funds is financially fair and reasonable.

With the blockchain techniques establishing the flow of funds, transparency and trust within the loosely affiliated group are enhanced, which builds a better future for this insurance model. BLockchain also provides a tamper-proof information disclosure which leads to better self-regulation, improves system availability and reduces management cost.



Usage mode

Hyperledger Fabric Usage Mode


Consortium Operator Oraganization
CA
Orderer
Consortium Administrator
Business Participant Organization
CA
Participant User
Participant Administrator
Alibaba Cloud BaaS
Participant User
Participant Administrator
Business Participant Organization
CA
Ledger
Chaincode
Peer
Channel
Peer
Ledger
Chaincode

Consortium Chain

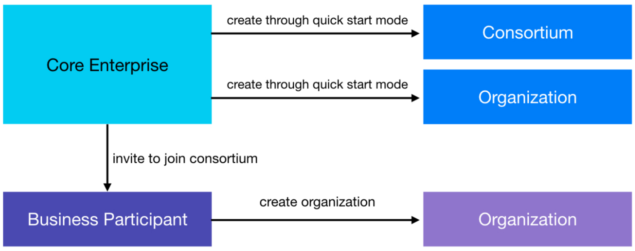
Alibaba Cloud BaaS provides two usage modes. Enterprises can select a mode based on their business specific.

> Note: The following information is for reference only. There is no strict boundary between these two usage modes, and you can choose one mode based on your needs.

Quick mode

If the business consortium is started or dominated by a key enterprise, and other businesses involved are invited to join the consortium, you can choose the quick mode.

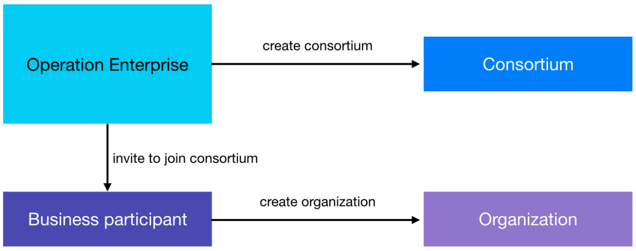
In the quick mode, key enterprises can quickly start their services on the blockchain and add more business participants to the consortium blockchains and business channels later. In this mode, the key enterprises can be both the operator and the participant, while other enterprises act as business participants.



Standard mode

If the consortium infrastructure is operated by a commissioned enterprise, and if other enterprises participate in business collaborations and transactions, you can choose the standard mode.

In the standard mode, the operator creates the consortium and invites other enterprises to join the consortium blockchain and the corresponding channels. In this mode, the enterprise in charge of operation acts as the consortium operator only (not the business participant), while business enterprises act as the participants.



Basic terms

General terms

Bitcoins

The first major applier of blockchain technology was Bitcoin, a world-renowned form of electronic cash created in 2009 by Satoshi Nakamoto.

Blockchains

Blockchain was first introduced to the market as the technology underpinning Bitcoin exchanges, but its practical uses in the business world extend far beyond cryptocurrency transactions. Blockchain establishes a peer-to-peer network where each participant in the network has access to a shared ledger. Transactions and history records cannot be removed or altered. The smart contract and consensus algorithms enable multiple participants to transact with one another and confirm the transactions and ledger records. Currently, Alibaba Cloud supports three types of blockchains: public blockchains, private blockchains, and consortium blockchains. Blockchain frameworks include Ethereum, EOS, Hyperledger Fabric, and Corda.

Smart contracts

As one of the highlights of blockchain technology, the smart contract describes the contract terms, the conditions of a transaction, and the business logic of transactions using cryptography. Smart contracts support self-execution and automatic reconciliation in real time.

Genesis block

The first block in a blockchain.

Hyperledger Fabric specific terms

Organizations

Organization refers to entities involved in the blockchain business network, such as enterprises, government agencies, and groups. Within the Hyperledger Fabric framework, each organization has one or more blockchain nodes, such as orderer nodes, peer nodes, and CA nodes. Alibaba Cloud blockchain service supports two types of organizations:

- The consortium operator manages and operates the public infrastructure of the consortium. An organization from the consortium includes the following types of node:
- CA: The Certificate Authority (CA) is an entity that issues digital certificates. CA provides users of a blockchain with a number of certificate services, including services related to user enrollment and transactions invoked on the blockchain.
- Orderers: An orderer is a node running the communication service that provides delivery guarantees. The orderer provides ordering hints for block formation and consensus services.
- Business participants: The companies or enterprises in a consortium. Each enterprise can define one or more organizations, including the following types of node:
- CA: The Certificate Authority (CA) is an entity that issues digital certificates. CA provides users of a blockchain with a number of certificate services, including services related to user enrollment and transactions on the blockchain.
- Peer: A peer receives ordered state updates from the ordering service and maintains the state and the ledger. Peers can also facilitate smart contracts and act as an endorser.

Consortia

A consortium is a collection of organizations involved in a blockchain-based business collaboration or a business transaction network. A consortium may consist of multiple organizations.

Channels

Channels are used to isolate the businesses in the consortium. Each channel represents a business and contains the participants of the business (some or all of the organizations within the consortium). There can be multiple channels in one consortium. One organization can join multiple channels. Each channel can be viewed as a sub-chain with its own ledger, and smart contracts can be deployed to the channel.

Chaincodes

A chaincode is a piece of code written in one of the supported languages such as Node.js, Go or Java. In the Hyperledger Fabric framwork, chaincodes are the ‘smart contracts’ that run on the peers and create transactions.

Orderers

An ordering service node that provides services to order and broadcast transactions. The orderer collects transactions from network members, orders the transactions and bundles them into blocks. The orderer delivers the block to all peers to ensure that ledgers are updated with the same transactions in the same order.

Peer nodes

Peer node: A node that maintains a ledger under the Hyperledger Fabric framework. Nodes in peer-to-peer networks must come to a consensus on the ledger status. There are two types of peers: endorsing peers and committing peers. You must install the chaincode on each endorsing peer node to forward the endorsement request to that peer. With no need to install chaincodes, the committing peer validates the transaction, accepts blocks of valid transactions from an ordering service, and persists the block information to a modular data store.

Anchor peers

The anchor peer serves as the entry point for the peer from another organization on the same channel to communicate with each of the peers in the anchor peer’s organization. The anchor peer in Hyperledger Fabric framework ensures high availability and keeps the entire network in a synchronized state.

Ant Blockchain specific terms

Roles

There are two types of roles:

- Consortium administrator is responsible for issuing applications for creating a consortium, has administrative right of the consoritum, and can invite other participants to join.
- Consortium participant can independently access a consortium to read/write data.

Ledger Data

Since data on blockchain is trustable and immutable, it is used as attestation for text or files, in form of a string or a hash of file contents.

Certificate Signing Request

CSR (Certificate Signing Request) is generated with tools like openssl. During the generation there will be two secrets, one is public key, i.e. this CSR, and the other is private key. Users should store private key and its password properly.

Private Key

Private key is generated with tools like openssl. During the generation there will be two secrets, one is public key, and the other is private key. Users should store private key and its password properly.

Certificate

Certificate is issued by Certificate Authority (CA) which has a partnership with Alipay. Users need to issue CSR for a certificate.

Private and Consortium Blockchain

The blockchain created or managed by a user.

Node Information

Information about a blockchain node. The total number of nodes for a blockchain is 3f+1, where f is a positive integer.

Business Classification

The type of business data schema of the transaction.

Reference Count

The number of transactions referenced by current transaction.

Business Time

The time for transaction submission.

Enterprise Ethereum - Quorum specific terms

EVM

Ethereum Virtual Machine, the decentralized computing platform which forms the core of the Ethereum platform.

Solidity

Solidity is a high-level smart contract programming language whose syntax is similar to that of JavaScript and it is designed to compile to code for the Ethereum Virtual Machine.

Gas

Gas is a unit to measure how much work is needed for executing a transaction, and depends on the number of steps or the complexity of the steps that a transaction has.

network id

A number which identifies a particular version of the Ethereum network.

geth

Ethereum client implemented in the Golang programming language

Dapp

Decentralized application.

Private transaction

Transactions whose payload is only visible to the network participants whose public keys are specified in the privateFor parameter of the Transaction.

Quorum node

A fork of geth, with modifications like:

- Consensus algorithms like Istanbul BFT or RAFT
- P2P layer for permissioned nodes
- Block validation logic for private transactions
- Removal of Gas pricing (but preserving Gas)

Transaction manager

Quorum's Transaction Manager is responsible for Transaction privacy. It stores and allows access to encrypted transaction data, exchanges encrypted payloads with other participant's Transaction Managers but does not have access to any sensitive private keys. It utilizes the Enclave for cryptographic functionality. The Transaction Manager is restful/stateless and can be load balanced easily.

Enclave

The Enclave works hand in hand with the Transaction Manager to strengthen privacy by managing the encryption/decryption in an isolated way. It holds private keys and is essentially a "virtual HSM" isolated from other components.