

浅谈区块链中间件系统设计

Ling

2019. 10. 26

CONTENTS



区块链与中间件

区块链简介

区块链的特征与特性

智能合约

中间件

区块链分类



Libra的中间件

LibraIDE

架构与设计原则

基础模块



中间件的一些看法

中间件的一己之见

中间件与底层

中间件与跨链

区块链

- 区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。
- 它本质上是一个去中心化的分布式数据库。任何人只要架设自己的服务器，接入区块链网络，都可以成为这个庞大网络的一个节点。

从谈恋爱到区块链



- 假如你是一个女孩，某年某月某日你男朋友对你说了一句“我爱你一生一世”。
- 然后你把这句话发给你的闺蜜，爸妈，朋友圈，微信群，知乎。你男朋友再也无法抵赖，因为大家知道了。
- 然后你个上述的这些一些红包，当作“矿工费”。
- “我爱你一生一世”这句话说话的时间，说话的对象等打包起来，形成信息包同步就是区块。
- 朋友圈，微信群等就是节点。如果男朋友不承认说过，你就找到这个账本对质，并且把男朋友节点踢出网络。

区块链与信息

- 在区块链系统里，有一本帐本(ledger)，它是一个电子档案，记录着所有的交易纪录。
- 所有节点同步到最高区块之后，会有大家所有的账本信息。
- 这帐本不是存放在一个中央机构（比如银行），或者一个数据库。它拥有无数份副本，散布存放在区块链网络上的每一台电脑里，而每台电脑我们称为“节点(node)”。
- 说到这里，关于帐本是由一组电脑共同维护，而不是由一个类似单一的数据库的中心机构来掌管，

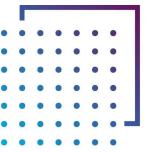
智能合约

- 智能合约是区块链上可以运行的程序。
- 是一套以数字形式定义的承诺，承诺控制着数字资产并包含了合约参与者约定的权利和义务，由计算机系统自动执行。

智能合约

区块链在早期是无法编程的，而账本（ledger）只能作为类似于分布式数据库的作用。

有了智能合约后，可以更有效的利用区块链技术，在各行各业的领域中落地，优化流程，共享数据。



中间件

中间件（Middleware）是处于区块链底层架构和应用程序之间的软件

中间件屏蔽了底层操作系统的复杂性，使程序开发人员面对一个简单而统一的开发环境，减少程序设计的复杂性，将注意力集中在自己的业务上，不必再为程序在不同系统软件上的移植而重复工作，从而大大减少了技术上的负担。中间件带给应用系统的，不只是开发的简便、开发周期的缩短，也减少了系统的维护、运行和管理的工作量，还减少了计算机总体费用的投入。



中间件的极简定义

中间件 -- 将具体业务和底层逻辑解耦的组件。

大致的效果是：

需要利用服务的人（前端写业务的），不需要知道底层逻辑（提供服务的）的具体实现，只要拿着中间件结果来用就好了。

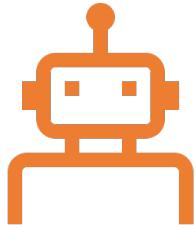
举个栗子

我开了一家金店（业务端），然而有不同的金矿（底层），为了成本我肯定想一个比价，再综合质量挑选一家金矿合作（适配不同底层逻辑）。由于客户需求，合作一段时间后，或许我需要用新的玫瑰金了。我又要重新和另一家金矿合作，进货方式、交易方式等等全都要重来一套（重新适配）。

然而我只想好好做首饰，有不同的标准化的金块送来就行。于是我找到了一个专门整合销售金块的第三方代理（中间件），跟他谈好价格和质量后（统一接口），从今天开始，我就只需要给代理钱，然后根据需求拿到金块就行。

节约用户边际成本，加速区块链应用落地。

区块链的分类



公有区块链（以Eth为首的，所有人都能参加，单独节点不受监管）



联盟链（国内主推的区块链技术，以行业或者联盟为基础，可以监管，信息透明，内部预选节点作为记账人）



私有链（单独节点，一般用于内部开发和调试）

无论是公链还是联盟链，都可以也需要中间件。

ChainIDE

跨越区块链的时间魔法

The World First Cross-Chain online Integrated Development Environment
For Ant Blockchain



IDE·背景

- ◆ IDE是指「集成开发环境 Integrated Development Environment」，是软件开发中必不可少的工具。在软件开发中一般都会包含代码编辑器、编译器、调试器等工具，
- ◆ 如给苹果设备开发 App可以使用苹果提供的 Xcode，给微软生态开发软件可以使用 Visual Studio系列等。

LibraIDE (www.libraide.com) 就是专为Libra Move量身打造的云端区块链IDE。

区块链开发环境·背景



随着智能合约的诞生与流行出现了大量开发需求，很多区块链项目更多的专注自己的底层开发，忽视了智能合约开发环境的便捷性。为开发者增加很多门槛和边际成本。

以Libra为例，在正常的网络环境中准备 Move可编译的环境至少需要 1小时，而且当前也只支持 macOS和 Linux。

ChainIDE 简介·背景

- ◆ 「ChainIDE」是全球首款专为区块链平台打造的多链代码编译工具，只需要 Web 浏览器就可以进行智能合约的编写，并由云端进行编译和部署，也是第一个「云端的多链IDE」。
- ◆ 目前已支持包含Libra在内的接近个区块链底层的环境编译，可以用于任何需要编写智能合约的场景，包括游戏、DeFi，去中心化应用的开发。



痛点描述·Libra为例



Facebook的Libra项目的愿景是为地球上仍然接触不到银行的17亿人民，提供便捷的金融服务，多方计算，去中心化应用等等。而Move语言是由Libra提出的全新的计算机编程语言。



Move是个很特殊的语言，它的语法是全新的。它继承了C和Rust语言体系的一些特性。同时也有些内置语法，比如move，copy等等，这些是更加方便编辑智能合约使用的。它同时也可以写递归和复杂逻辑，使用起来比现有的智能合约语言更加顺畅。

页面展示·MOVE(例)

ChainIDE - Swift,Simple,Smart

First OnlineIDE support MOVE, IOST & ETH
Build your DApps with us
Today's progress was yesterday's plan

Try it now

MOVE IOST ETH

```
contract.js
class Bet {
    constructor(player_amount, numbers, player_seed, hash, inviter) {
        this.amount = player_amount;
        this.host_hash = hash;
        this.player = player;
        this.player_seed = player_seed;
        this.host_seed = "0000000000000000";
        this.wyvideoTrack;
        this.wyhttpRequestEventTarget;
        this.revealsWebsocketTrack;
        if (!player_amount)
            throw new Error("Player amount is required");
        if (!numbers)
            throw new Error("Numbers are required");
        if (!player_seed)
            throw new Error("Player seed is required");
        if (!hash)
            throw new Error("Hash is required");
    }
    reveal() {
        const crypto = IOSTCrypto;
        let sum = 0;
        for (let i = 0; i < hash.length; i++) {
            sum += hash.charCodeAt(i);
        }
        return sum % 100 + 1;
    }
}

dice.js
class Dice {
    constructor(strong, string, strong, string, string) {
        this.strong = strong;
        this.string = string;
        this.strong = strong;
        this.reveal = reveal;
        this.del = del;
    }
    reveal() {
        if (!this.strong)
            throw new Error("Strong is required");
        if (!this.string)
            throw new Error("String is required");
        if (!this.strong)
            throw new Error("Strong is required");
        if (!this.reveal)
            throw new Error("Reveal is required");
        if (!this.del)
            throw new Error("Del is required");
    }
}
```

由于Move语言的特殊性，上来就给试用者设置了很高的门槛去初始化环境，是非常不友好的。通过我们的IDE工具，可以在3秒内成功编译一份Move的合约，大大节约了用户的时间，降低了开发者的进入门槛。

在物理世界中时间是无法操纵的，而在代码时间里，我们可以帮助全球的开发者节约边际成本。ChainIDE 的出现，无疑帮助了成千上万的教授，设计师、开发人员节约了这 1 小时无意义的边际成本。

1分钟内可以写出自己的 Move程序，这是时间的魔法”

by Ling

Inspired from Stadia



页面展示·ChainIDE

The screenshot shows the ChainIDE interface. At the top, there's a navigation bar with 'BaaS' and 'WM-Test1'. Below it is a tabs section with 'Transactions', 'HelloWorld.sol', 'HelloWorld.sol', and 'Welcome'. A 'Deploy HelloWorld' button is visible. The main area contains a code editor with the following Solidity code:

```
// Constructor code is only run when the contract
// is created
constructor(string initMessage) public {
    message = initMessage;
}

// Updates message variable
function set(string newMessage) public {
    message = newMessage;
}
```

On the left, a sidebar shows deployment details: From: 0x126c85fc5d7ab0b37defaadefb67e8e3e5b2d0f4c43f545b75d3c978c7180; To: <HelloWorld:WM-Test1:uotb3dmudw>; Age: 3 sec; Block #15117281 (Index). Below that is another 'Deploy HelloWorld' section with similar deployment details. The bottom part of the interface shows an 'Output' window with deployment logs:

```
14:04:38 Using Solidity compiler version BaaS solc 0.4.20
14:04:39 Success in compilation
14:04:41 Deploying contract
14:04:46 Transaction hash: 0x5206c6fb5538616b12eea7351330a7d6641213c85fe32ef4bf3e5f76421aa93
14:04:46 Contract deployed at block number: 15117249
14:05:06 Getting value ...
14:05:13 Get value success.
14:05:35 Calling contract function...
14:05:35 Failed, something was wrong
14:05:43 Failed, something was wrong
14:05:43 Failed, something was wrong
14:05:54 Calling contract function...
14:05:57 Function call succeeded at block number: 15117281 with transaction hash: 0x8ad42ccf63f028e04132875c10149dad553e6a6e9b6d1d749615b566722bc28
```

闪电快速

比普通编译器快10倍。一个真正的黑客IDE，帮助设计师做敏捷开发。

使用方便

一键来完成设计/编译/测试/部署/调用。在3秒内将编码员带入区块链世界。

功能完善

单击生成所有功能树满足编译要求

重量轻盈

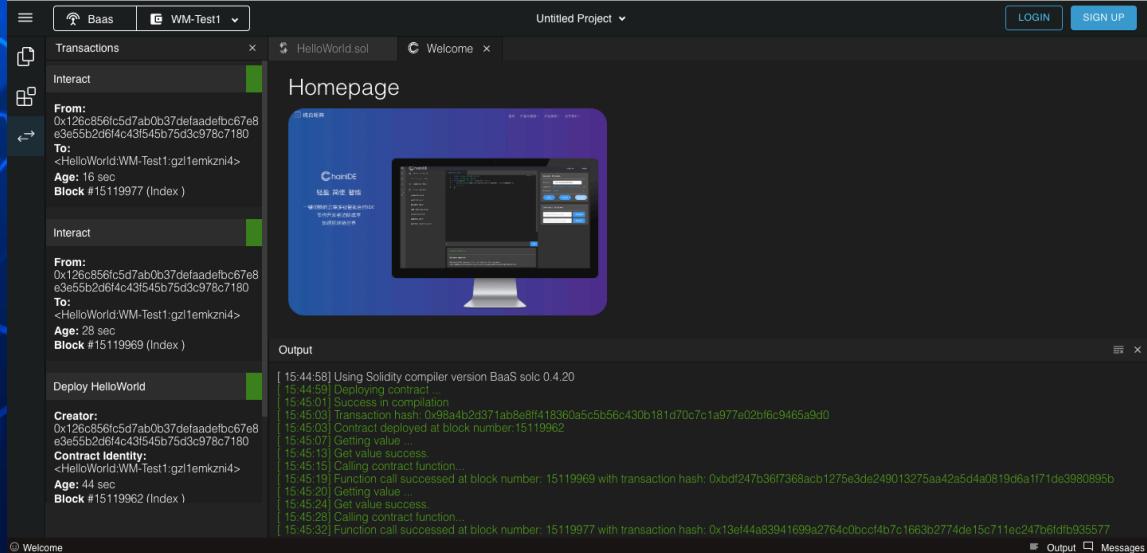
无需下载或编译，所有基于Web的在线IDE。

服务贴心

完全免费且提供24/7小时在线支持和个性化服务



ChainIDE·融合 联盟链与公链



蚂蚁区块链 BaaS (Blockchain as a Service) 平台是蚂蚁金服自主研发的具备高性能、强隐私保护的金融级区块链技术平台。平台致力于打造一站式服务，有效解决金融、零售、生活等多场景区块链应用问题。通过更加可靠，安全，高效的平台服务，使合作伙伴可轻松搭建各类业务场景。

ChainIDE for AntFinanceBlockchain为所有的开发者提供一个0门槛上手的体验通道。只需要完成智能合约的编写，就可以一键在Libra的体系内进行编译、部署、调试。当开发者MVP开发完成，未来等待Libra主网上线，我们也会提供一键并入主网的服务。

ChainIDE·应用展示

Java SDK

版本号	功能更新	对应链版本	下载链接	SDK 使用说明
0.10.2.9	<ul style="list-style-type: none">- 支持查询关联交易的 depositFlag;- 修改监听 topics 接口；- 新增批量查询交易和收据接口；- 更新黑名单接口；- 添加 WASM 示例；- 密码学支持包括 SM2、R1 等；- zoro 依赖包支持至 0.0.4 版本。	V0.10.2.7.1 V0.10.2.9.1 V0.10.2.9.2	点击下载 SDK	查看 Java SDK 开发指南
0.10.2.4	- 支持合约平台所有客户端功能。	V0.10.2.4.7	点击下载 SDK	查看 Java SDK 开发指南

JS SDK

版本号	功能更新	下载链接	SDK 使用说明
0.2.27	<ul style="list-style-type: none">- 支持 TLS/HTTPS 协议；- 支持账户合约操作、查询、事件订阅等功能；- 支持 Solidity 和 C++ 合约。	点击下载 SDK	查看 JS SDK 开发指南

C++ SDK

Java SDK Requirements

JDK 7+

Maven 3.5.4+

在 Linux 下使用 SDK , 要求 GLIBC 版本高于 2.14

Js SDK Requirements:

Node.js v10.11.0 +

JS SDK

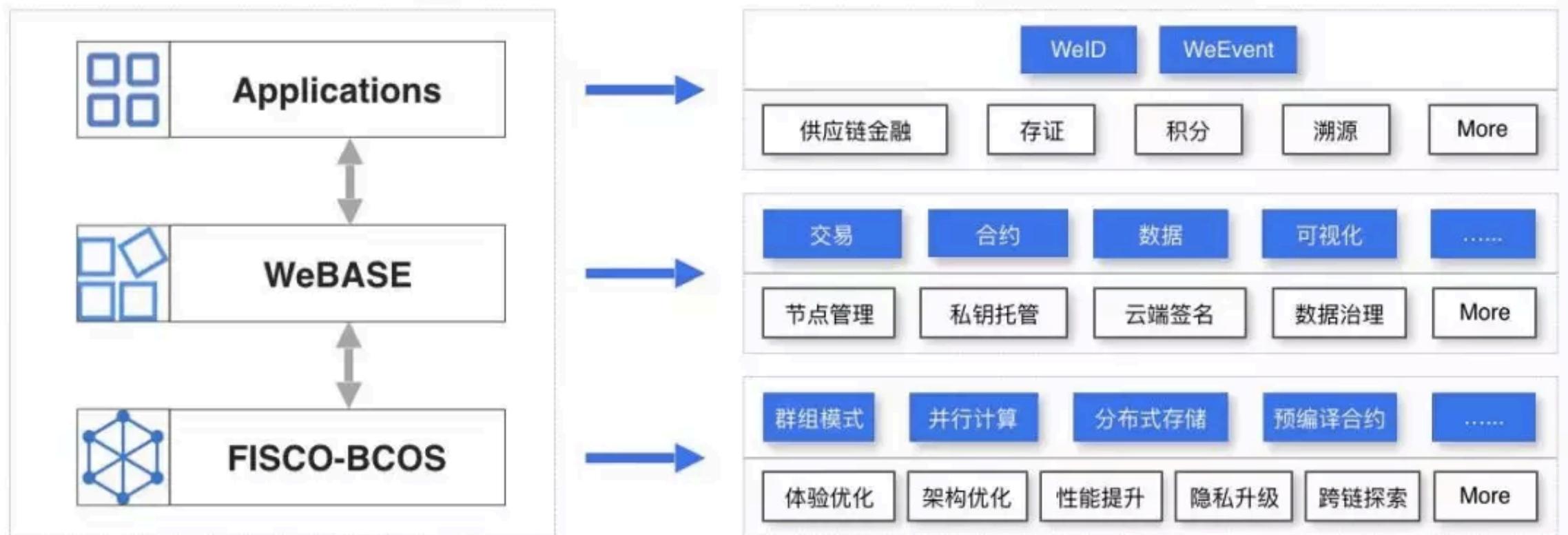
...

如果使用ChainIDE , 不需要任何环境配置 , 只要点击一次即可完成编译部署。

不同中间件的设计理念

什么是WeBase?

- 微众银行正式开源自研的区块链中间件平台——WeBASE (WeBank Blockchain Application Software Extension)是区块链应用和FISCO BCOS节点之间搭建的中间件平台，该平台适配支持FISCO BCOS底层平台，面向多种对象，如开发者、运营者，并根据不同的场景，包括开发、调试、部署、审计等，打造丰富的功能组件和实用工具，提供友好的、可视化的操作环境。



设计理念



按需部署

WeBASE组件不需要全部部署，根据需求部署应用所需要的组件。



微服务

WeBASE采用微服务架构，提供Restful风格接口。



零耦合

所有子系统间零耦合，均可独立部署，独立提供服务。

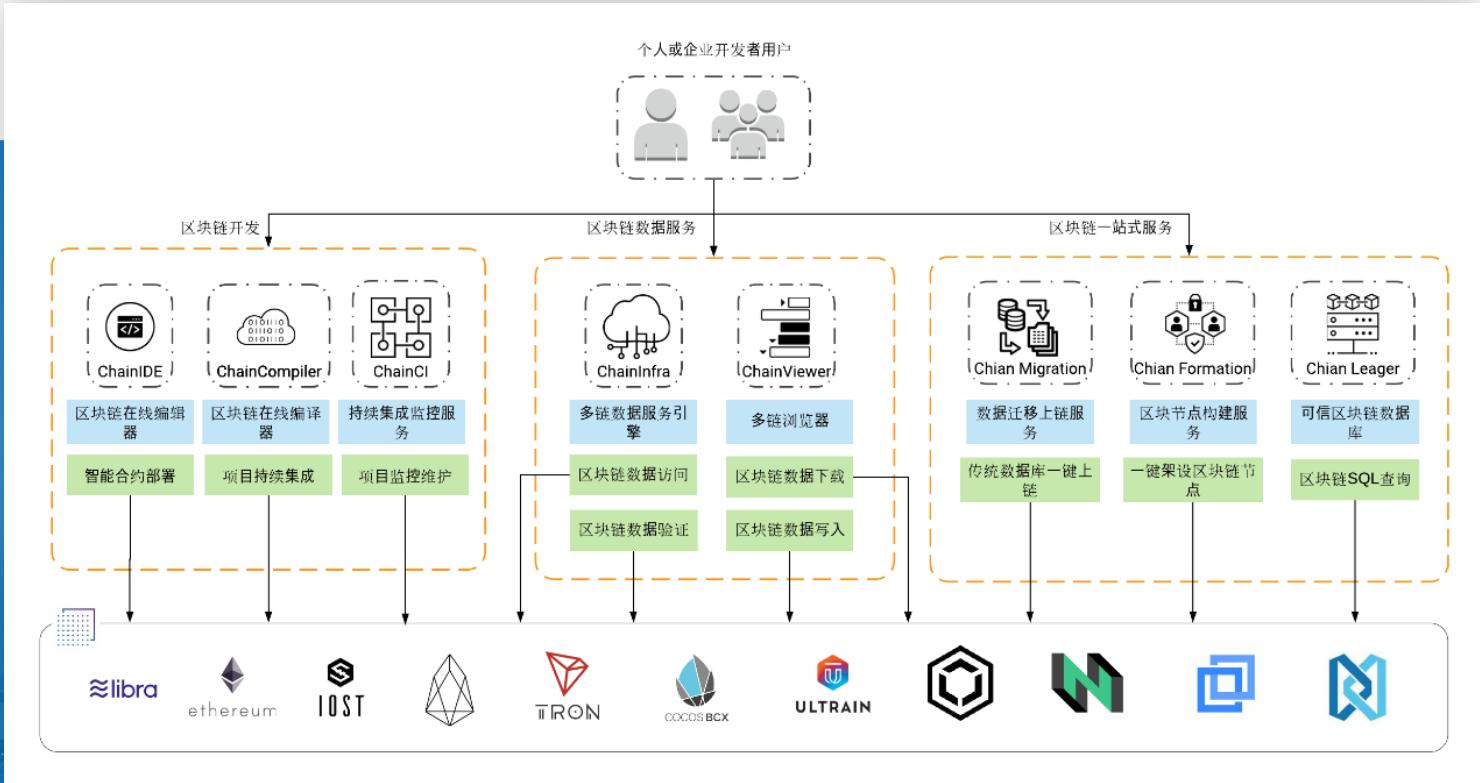


前后端分离

开发者可以使用后端接口，定制自己的前端页面。



技术架构

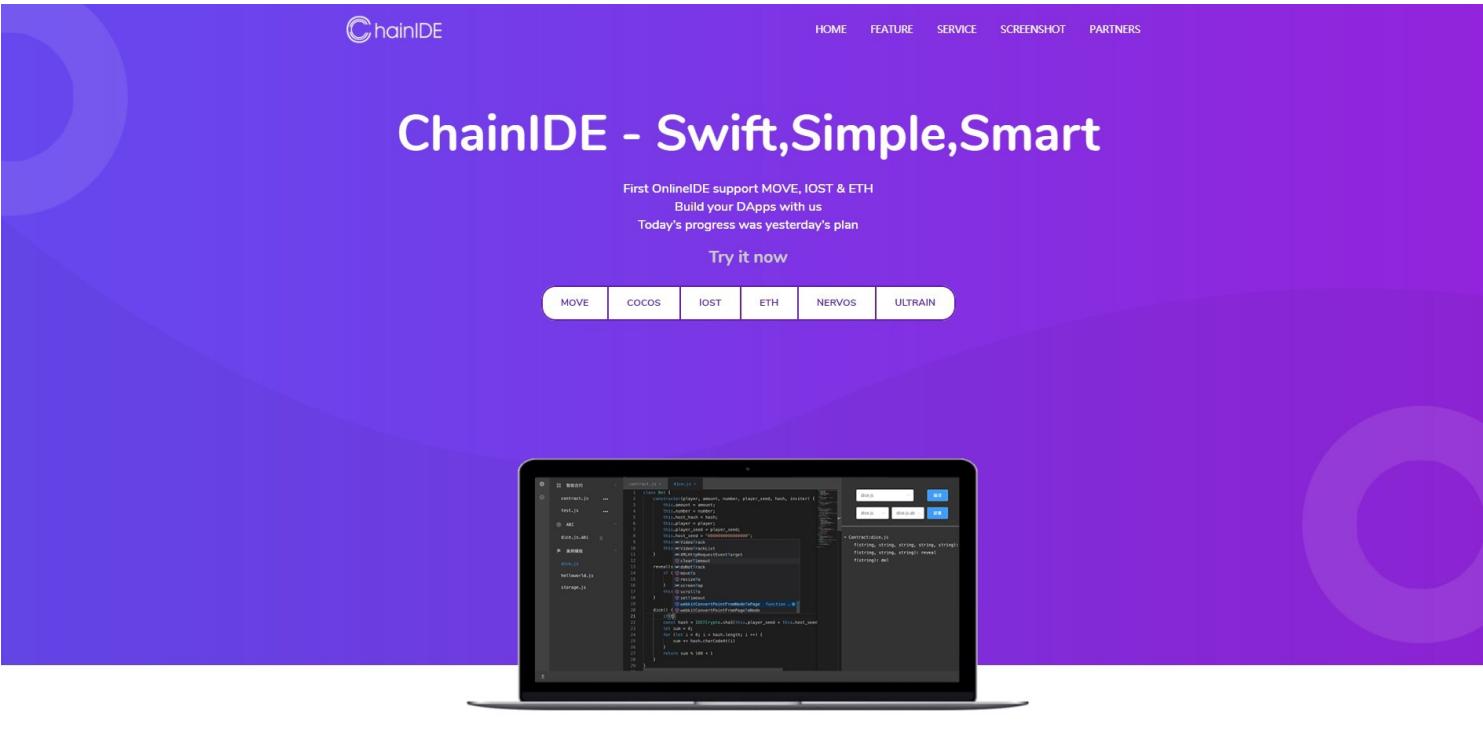


多链中间件ChainIDE生态

ChainIDE可以零门槛全平台调试多链的在线编译环境，无需任何环境搭建与区块链配置。该产品已经帮助全球超过100个国家开发者编译50万份智能合约，40万次的教学服务是全球区块链最大的开发者流量入口之一。ChainIDE还提供了全套自研生态工具，IDE，测试网，内置钱包，浏览器，教程等体系化的提供一站式服务，全方位的为智能合约设计保驾护航，节约开发者边际成本，加速区块链应用落地。



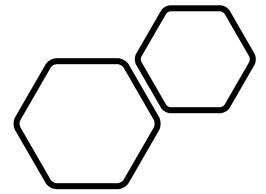
ChainIDE与中 间件生态



ChainIDE

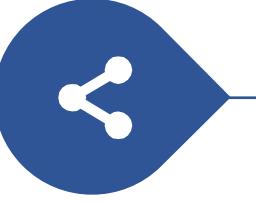
云端智能合约开发工具

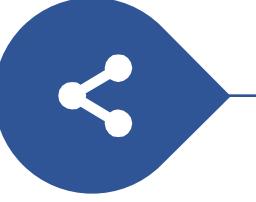
- 智能合约云端开发
- 0门槛上手
- 无需任何环境搭建
- 节约边际成本
- 加速区块链落地

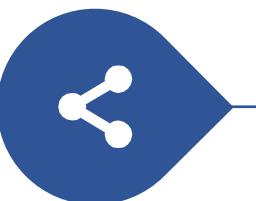


ChainIDE for Libra

(libraide.com)

-  **A. 适用型的突破**

通过通用的云后端，帮助各条区块链突破他们的适用型限制。
-  **B. 可拓展性的延伸**

方便快捷的帮助开发者把他们的智能合约，DApp以及数据一键同步到对应网络，大大提升了各大区块链的拓展性
-  **C. 便捷性的具现**

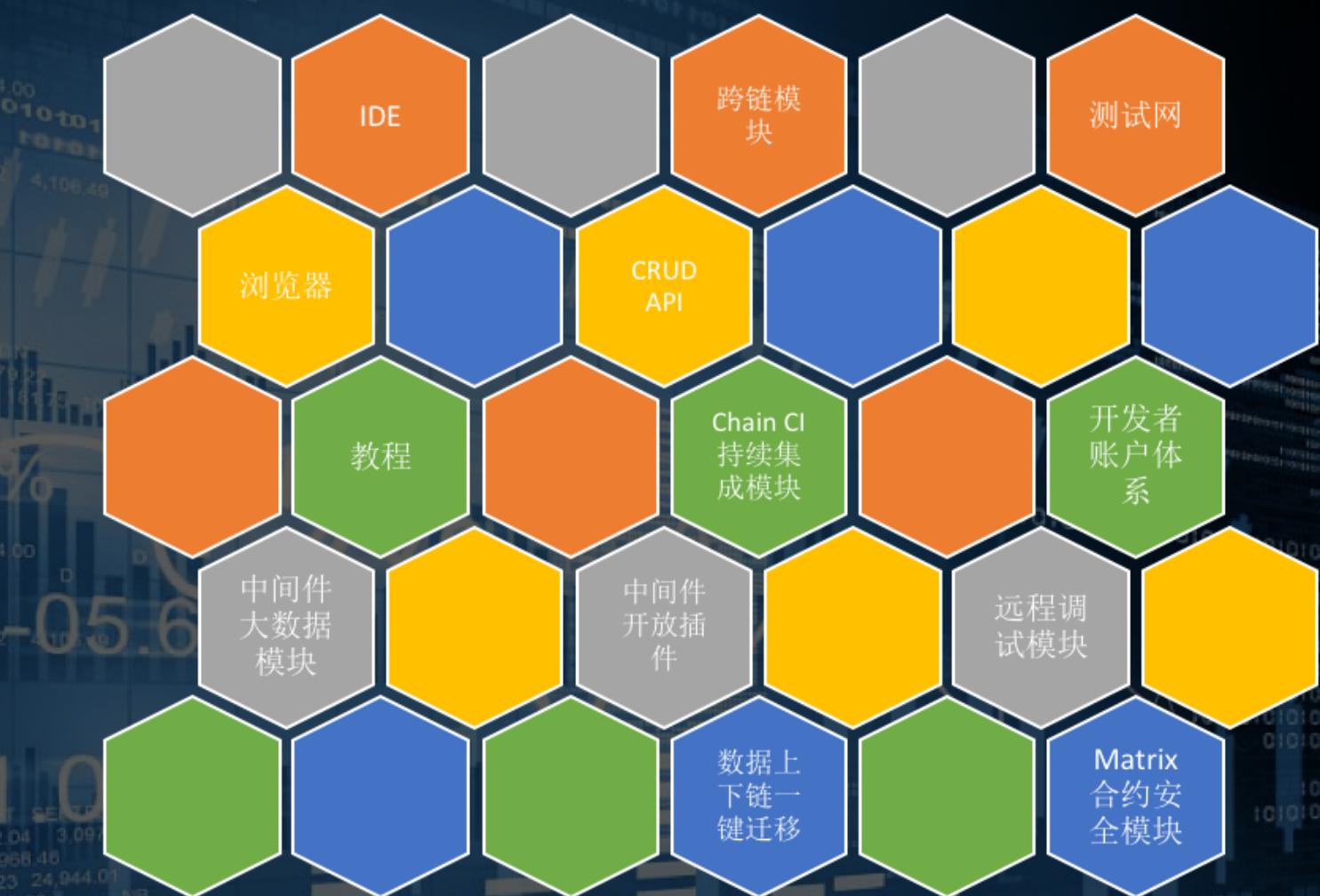
ChainIDE可以快速的帮助全球的开发者在不同的区块链项目，系统需求，编译环境和硬件基础完成0门槛的上手体验。

全套中间件 自研体系

25%

11.0

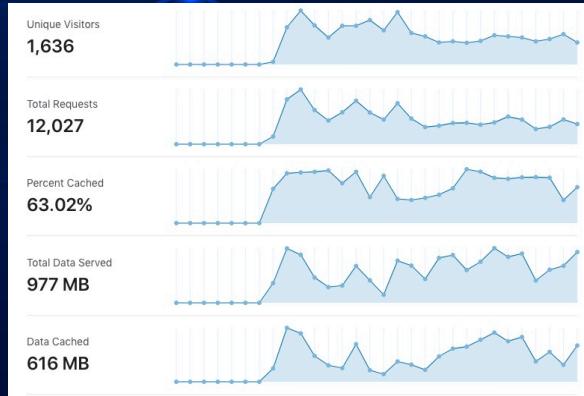
-05.6



影响·成就



Chain IDE



Eth IDE



Libra IDE



IOST IDE

数据方面

ChainIDE目前在编译次数，开发者DAU还有接入公链数量上来看都是最多的区块链IDE，已经有超过50万份合约通过我们的IDE编译。我们为全球超过100多个国家的开发者提供便捷的智能合约辅助设计，编译和调试服务。

影响·成就

媒体支持



央广网



网易新闻



人民网



中国网



巴比特

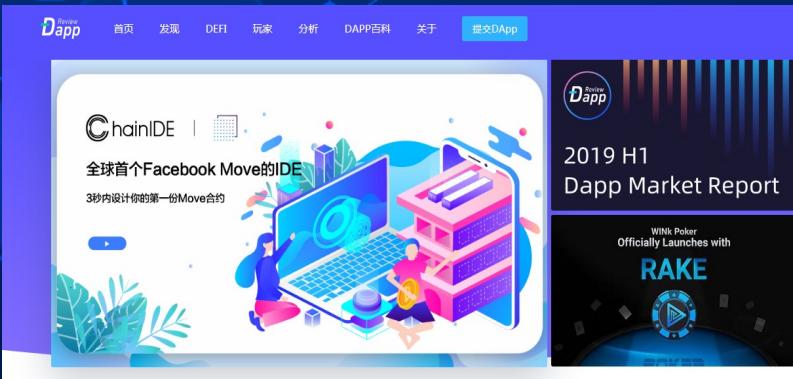


CSDN

影响·成就

社区推荐

DappReview首页推荐



合作节点

IOST发布支持Facebook Libra的Move语言IDE

据IOST官方消息，IOST节点合伙人纯白矩阵为IOST打造的ChainIDE成为全球首个接入Facebook Libra的云端IDE。该工具可以Libra上基于Move编程语言的智能合约和IOST智能合约间的一键转化，也可实现项目间DApp的便捷共享。



Libra Community

Github



香港中文大学（深圳）软件与区块链系统实验室

Software and Blockchain Systems (SFENKS) Laboratory, CUHK-Shenzhen

简体中文

English



BLOCKCHAIN

CLOUD-EDGE

GAME

TALKS

MEMBERS

ABOUT

RESOURCES



News

[Game Research Seminar] Towards Emotion-Based Adaptive Games: Emotion Recognition Via Input And Performance Features



Xiao Wu Delivered A Blockchain Game Talk At CUHK-Shenzhen



Prof. Cai Has Been Elected As A Committee Member Of CCF Technical Committee On Blockchain

2018-11-28



Chaojie Zhu From Carnegie Mellon University Delivered A Game Engine Development Talk At CUHK-Shenzhen

2018-11-22



Prof. Cai Delivered A Keynote Speech Titled "Connecting Blockchain And IoT Applications With Payment Channels" At BlockSys2018

2018-11-04

Ling

LingTian

[Edit profile](#)

An indie game developer. A SF writer. A DApp lover.

White Matrix

China & Canada

Organizations

[Overview](#)[Repositories 40](#)[Projects 0](#)[Stars 5](#)[Followers 21](#)[Following 1](#)[Data](#)[2048-multiplayer](#)

Forked from es/2048-multiplayer

Give it a try here:

JavaScript

184 contributions in the last year

[Contribution settings ▾](#)[2019](#)

2018

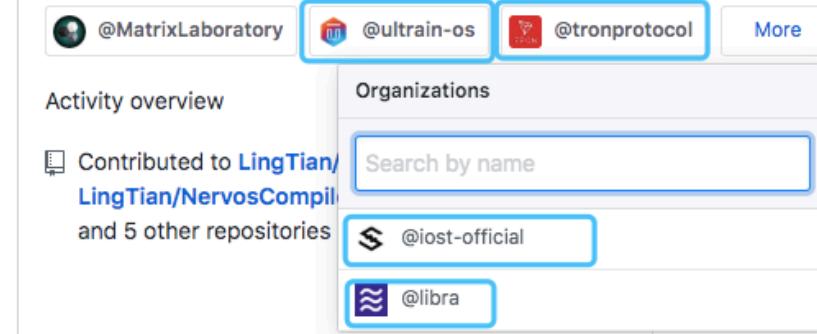
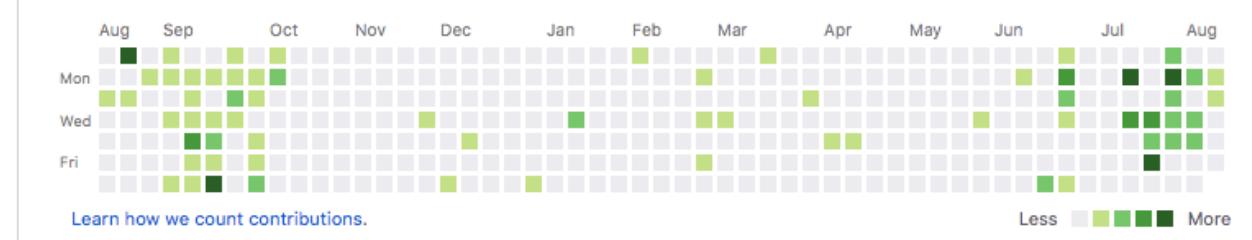
2017

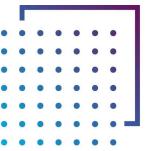
2016

2015

2014

2013





全套中间件自研套件

香港中文大学（深圳）软件与区块链系统实验室
Software and Blockchain Systems (SFENKS) Laboratory, CUHK-Shenzhen

■ 简体中文
■ English

BLOCKCHAIN CLOUD-EDGE GAME TALKS MEMBERS ABOUT RESOURCES

News [Game Research Seminar] Towards Emotion-Based Adaptive Games: Emotion Recognition Via Input And Performance Features

Xiao Wu Delivered A Blockchain Game Talk At CUHK-Shenzhen

Prof. Cai Has Been Elected As A Committee Member Of CCF Technical Committee On Blockchain
2018-11-28

Chaojie Zhu From Carnegie Mellon University Delivered A Game Engine Development Talk At CUHK-Shenzhen
2018-11-22

Prof. Cai Delivered A Keynote Speech Titled "Connecting Blockchain And IoT Applications With Payment Channels" At BlockSys2018
2018-11-04

libra LibraViewer VM-testNet

Search by Version / Address

Add #Addresses 31,210 TRD #TX Per Day 171 Transaction Amount 113,660 Total Supply 40,021,127,184,270

Latest Transactions

Version	From	To	Amount	Type	Expiration At
31210	607995ee68069a66a2a7ce08...		0	CUSTOM	12/18/2019, 3...
31209	77240ad0e3b72d1534f9012b...	1dd0c4dc10cd620f62801e7f...	16	PEER_TO_PEER_TRANSFER	12/18/2019, 2...
31208	33d4035d7a09db9927446493...	bc495191deb153dec64550aa...	25	PEER_TO_PEER_TRANSFER	12/18/2019, 2...
31207	92e3347ce7b19a972171219b...	4885af1beb238dbc24cc1686...	27	PEER_TO_PEER_TRANSFER	12/18/2019, 2...
31206	215387ce238609fb9965c1e2c7...		0	CUSTOM	12/18/2019, 2...
31205	884bef0c779e3e1fa81ddf8cca...	6320148b5690f441bdff1a141...	19	PEER_TO_PEER_TRANSFER	12/18/2019, 2...
31204	bc495191deb153dec64550aa...		0	CUSTOM	12/18/2019, 2...

ChainIDE

Start contract
contract...
Compiled file
publish...
Case template
transfer.mir
publish.mir
balance.mir
add_function.mir
recursion.mir
address.mir
payment_channel.mir

Network WM-TestNet(8b7b9a)
Address bc74d912d7dbb15626ef39f...
Balance 90000

Mint Create Import

Contract Actions
publish.mir
Compiled
publish.mir/complied
Execute

```
contract.mir >
1 import libLLVM;
2 import libLibra;
3
4 native move毁灭 amount: u64 {
5     LibraAccount!毁灭_to_address(amount);
6 }
```

Contract: publish.mir
public move毁灭 LibraAccount{T}; Self.T
public value(this:isSelf:T); u64
public destroy_t{T}(Self.T)

Check transaction details
Balance updated!
Balance updated!
Successfully updated the new balance for account: bc74d912d7dbb15626ef39fbc0e30ba

ChainIDE

First IDE support Facebook Move
Design your first move module today

Sequence Number: 276
Sent Event Key: 45d57336713b659eb268acf9b5361dfa6ebf8556f1988df94942c6cda980d46f
Received Event Key:
a346f9e19359171462cc232701594bd7b9d6bb328007e91d7332b514ebc772e0
Authentication Key:
607995ee68069a66a2a7ce08d8f58594af3c929dc6f6465d17330c1d9f8650b

Wallet Details

Network WM-TestNet(8b7b9a)
Address bc74d912d7dbb15626ef39f...
Balance 90000

Mint Create Import

chainCastle

About Move Why EN 中文

Move your Castle by Move
Learning Libra Move within 7 Days?
Let's try MoveCastle

START GAME → LEARN MORE →

IDE , 浏览器 , 开发者钱包 , 测试网 , 教程

科研成果 (2019)

1

Wei Cai and Xiao Wu, Demo Abstract: An Interoperable Avatar Framework Across Multiple Games and Blockchains, In 2019 IEEE Conference on Computer Communications Demos (INFOCOM 2019 DEMOS), Paris, France, April 29-May 2, 2019.

2

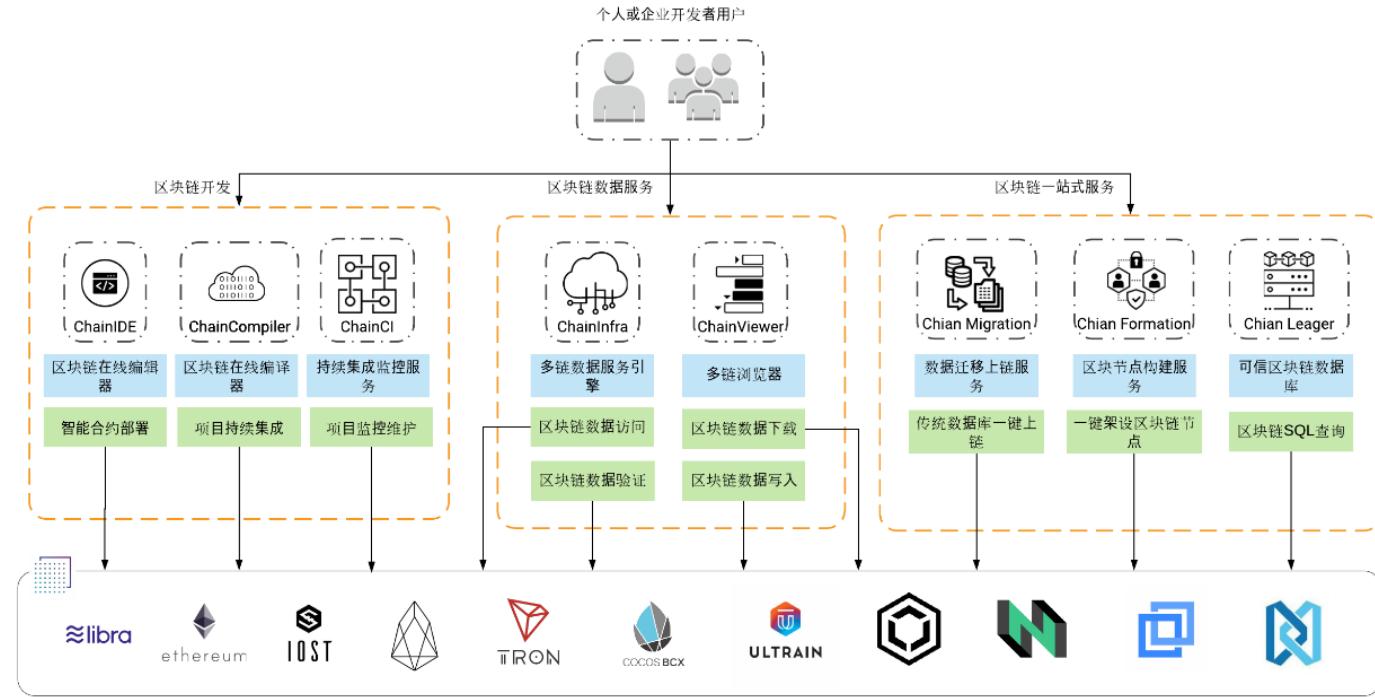
Tengfei Wang, Shuyi Zhang, Xiao Wu and Wei Cai, Rhythm Dungeon: A Blockchain-based Music Roguelike Game, In Foundation of Digital Games (FDG 2019), San Luis Obispo, California, USA, August 26-30, 2019.

3

Han Qiu, Xiao Wu, Shuyi Zhang, Victor C. M. Leung and Wei Cai, ChainIDE - A Cloud-based Integrated Development Environment for Cross-blockchain Smart Contracts, IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2019), Sydney, Australia, Dec 11-13, 2019.

4

Kun Xin, Shuyi Zhang, Xiao Wu, Victor C. M. Leung and Wei Cai, Reciprocal Crowdsourcing: Building Cooperative Game Worlds on Blockchain, In 38th IEEE International Conference on Consumer Electronics (ICCE 2020), Las Vegas, Nevada, USA, January 4-6, 2020.



关于中间件的一己之见

中间件可以兼容公链与联盟链体系。
节约边际成本，加速区块链应用落地。

中间件与底层

区块链底层战争

其实大多数区块链项目都是在打区块链底层的主意。因为现在区块链的性能不高是众所周知的。从公链的Eth上第一次能写程序，打开了区块链2.0的大门后，各种公链，联盟链都在尝试把底层做的更好。比如有些思考解决TPS的问题，包括优化算法，包括设计不同的底层结构等等。

区块链的底层战争其实打得只有一点，就是话语权。这是一个赢者通吃的局面。一旦一个好用的底层出现，无数应用都会选择它作为区块链的起始点，就和手机上的苹果与安卓系统一样。

联盟链性能更好

联盟链上的应用落地也许会更快

底层战争还没有结束

中间件与跨链

区块链并非互联网

现在有的区块链体系并非是互联网体系，因为互联网的信息是互联的。我们正常在任意区块链的系统里，是无法搜索到其他区块链里的信息的，无论是公链还是联盟链。简单来说现在应该是局域网的时代。跨链技术想要解决的问题是能够把区块链的信息在不同系统里也可以通过某种方式交互。

跨链问题还没有得到有效的解决。

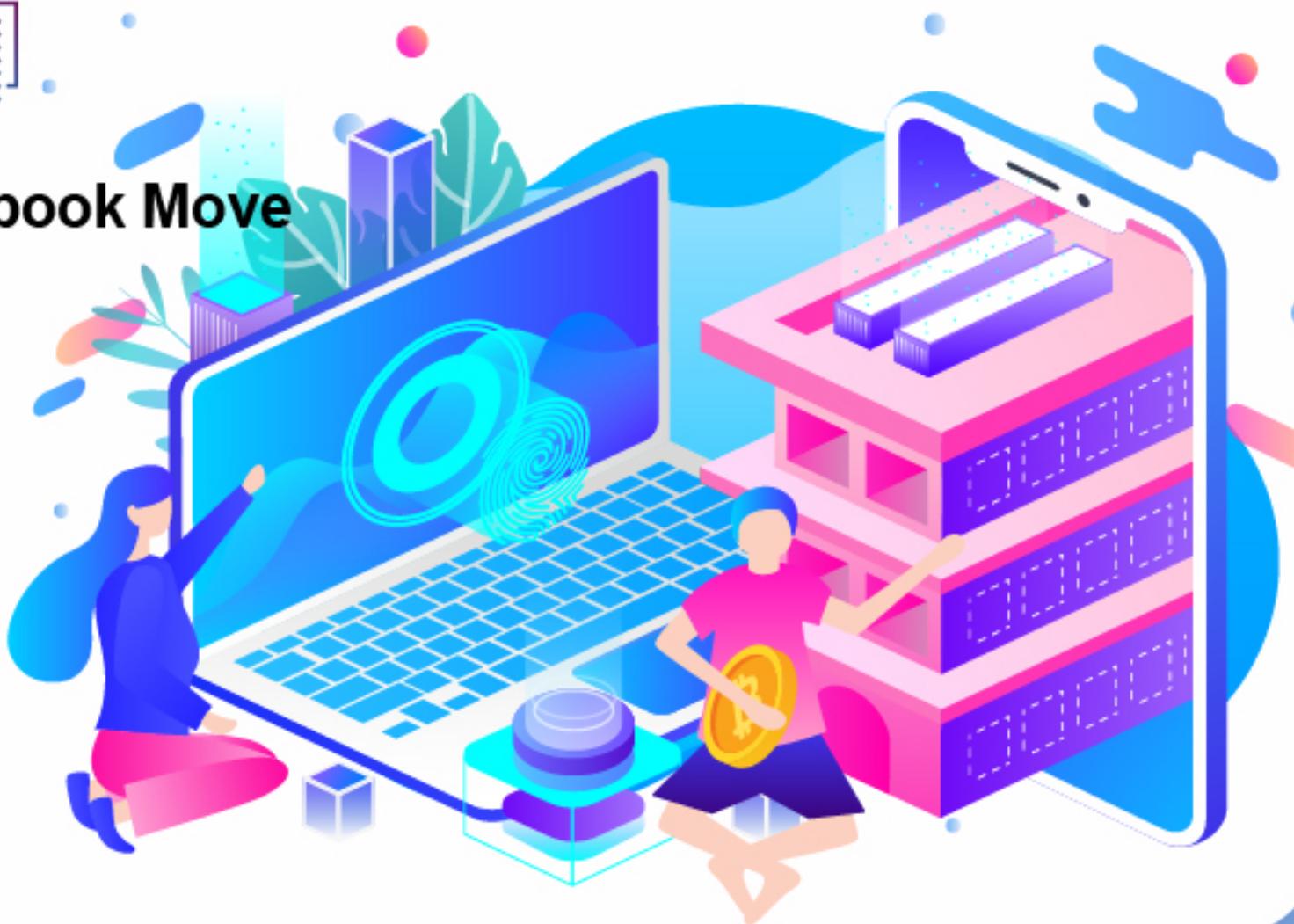
跨链在信息协同的体系里会有更大的作用。

ChainIDE



First IDE support Facebook Move

Design your first move module today



纯白矩阵

感谢您的观看

Present by Ling

