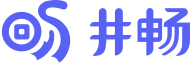
# 

Financial Industry

on

SWTC blockchain

Solution



Author: JingChange

Email: [jccdex@jccdex.com](mailto:jccdex@jccdex.com)

Index

[Preface 3](#_Toc627125480)

[System architecture 5](#_Toc248202884)

[System architecture overview 5](#_Toc1132628914)

[Node 6](#_Toc799110590)

[Consensus algorithm 6](#_Toc288957792)

[Financial blockchain 7](#_Toc1053084277)

[Software architecture 8](#_Toc1774708612)

[Overview 8](#_Toc1127268701)

[Payment 9](#_Toc904323873)

[Remittance 10](#_Toc1229563692)

# Preface

At present, the embrace of blockchain and business is getting faster and faster, and various applications are emerging endlessly. It is no longer a geek toy in the community, but various industries to explore and practice how blockchain technology is applied in business.

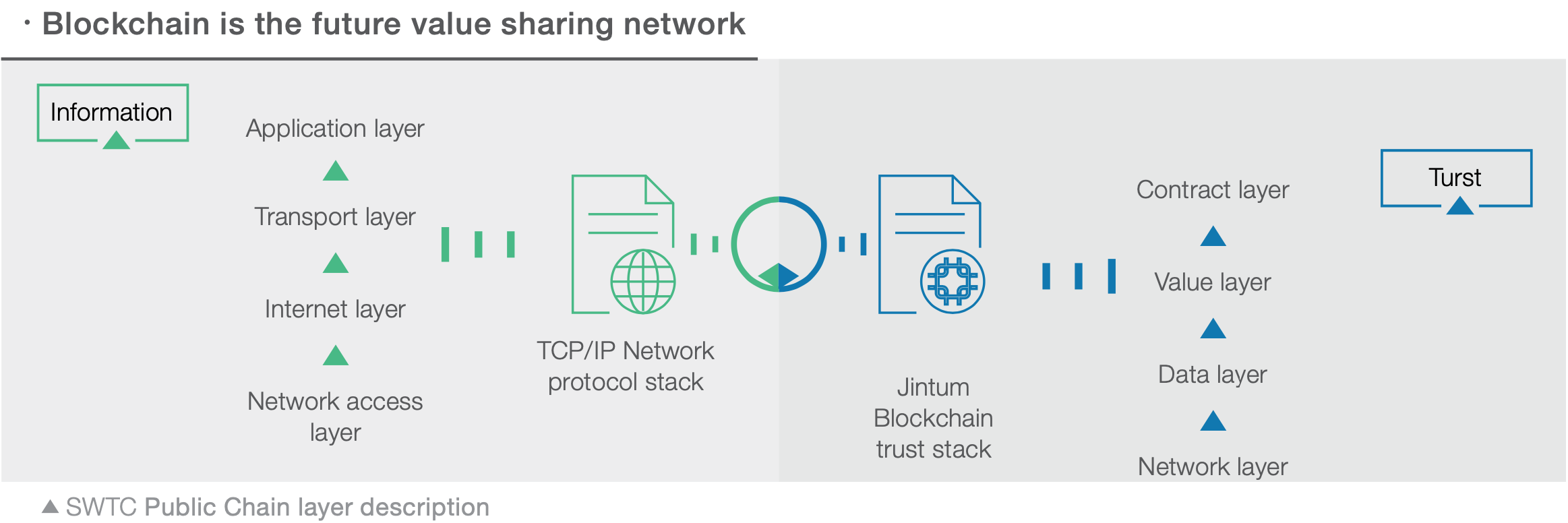
According to the characteristics of the financial industry, this manual explains how to deploy SWTC blockchain, how to interface with the legacy systems in the financial industry, and how to deploy and implement banking business based on blockchain technology now and in the future.

This article is based on a lot of information provided by [SWTC Foundation](http://www.swtc.top/), and I would like to express my gratitude.

Author: SWTC community [JingChang node](https://jccdex.cn) # SWTC blockchain

in 2011, Bitcoin was first introduced, and SWTC’s entrepreneurial team studied Bitcoin’s kernel technology “blockchain” as an emerging technology for changing the way of human society is organized in the future. in 2014, the SWTC Public Chain was launched to the market.

SWTC Public Chain had operated successfully for 5 years already, 12 million blocks height (as of May 2019), 5000 TPS in commercial public chain could be met. The vision of SWTC Public Chain is to provide a safe, valid, credible commercial blockchain environment. at the same time, The SWTC Public Chain is also positioned as a decentralized trading platform that accommodates a variety of digital assets.



Blockchain technology firstly solved data source from multiple parties to be trustable and allow different data assets could be transacted. it could help to prevent “double consumption” problem, which could greatly reduce the cost of mutual trust in multi-party and boost the sharing of value in low cost.

The SWTC blockchain is a trust machine.

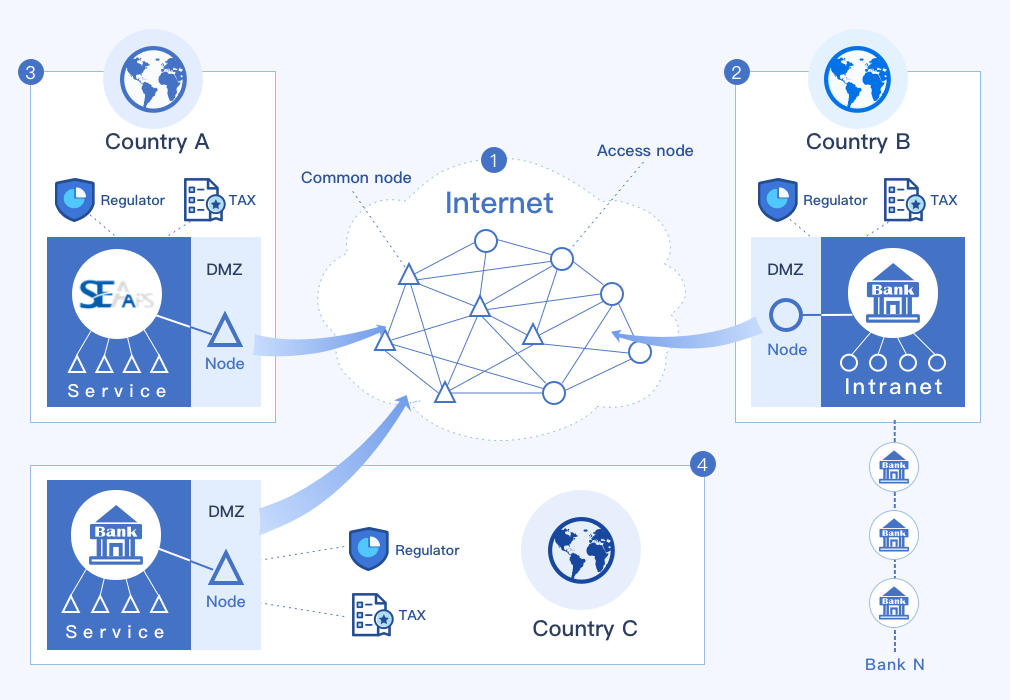
Comparison of Major Blockchain Technology Functions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Topic | BTC | ETH | Hyperledger | Ripple/Stellar | SWTC |
| consensus mechanism | PoW | PoW | DIP type | Consensus | RPBFT |
| Multi-assets | N | Contract | Contract | Native | Native |
| Asset exchange | N | Contract | Contract | Native | Native |
| Smart contract | N | Y | Y | N | Y |
| Performance | Weak | Weak | Good | Fair | Good |
| Number of nodes | Very much | A few | No public chain | Fair | Fair |

# System architecture

The blockchain in the financial industry is not a public chain and must meet financial regulatory requirements. Therefore, this requirement must be fully considered in the system architecture. This chapter must meet the matters that should be noted in the blockchain system architecture of financial services.

## System architecture overview



* Zone 1：Blockchain network is also a virtual network running on the Internet.
* Zone 2/3/4：The node zone in the blockchain network can be a single node or a mixed zone of nodes and business applications;
  + DMZ：Demilitarized zone, is located between two firewalls.It is usually recommended to deploy blockchain node services in this zone to connect the blockchain network and the internal business network;
  + SEAAPS: SEAAPS is applications which provides basic services for blockchain, such as blockchain browser, oracle service(Not a database service, but coordination of on-chain and off-chain data services);
  + Intranet/Service: Business application services are banks’ own internal business systems, such as bank account systems, KYC services, etc.
  + Regulator: Financial industry regulators to supervise transactions to meet anti-money laundering (AML) management needs;
  + TAX: Tax regulator；
* Triangle image：The consensus node representing the blockchain, usually the accounting node designated by the alliance chain management organization for election. Consensus nodes are responsible for voting and accounting.
* Circle image: access(public) nodes, nodes that the alliance chain allows access to, nodes without accounting rights

## Node

The SWTC blockchain is a virtual network connected by nodes of multiple participants. Each participant in the network can have one or more nodes. They exist in the form of network services, and each node maintains all Or part of the ledger data, there are multiple copies of the ledger data in the entire blockchain network, so single or part of the nodes will be disabled, no data will be lost, and the service will not be stopped.

The consensus protocol of SWTC Public Chain adopts randomized BFT. The core part of SWTC Public Chain contains several validating nodes that maintain the underlying validating network for the system. This network opens for every application on SWTC Public Chain access. DAPPs on SWTC Public Chain refer to the applications based on SWTC Public Chain for specific users. These applications can directly access to the public SWTC Public Chain through the API provided by the SWTC Public Chain. These applications can help to validate.

Two functions may be implemented:

1. it is involved in the consensus of public nodes in the network on the SWTC Public Chain.
2. if an application only uses aPi to access to the blockchain, there is no need to deploy a single authentication node.

The PBFT algorithm has a one-third fault tolerance rate, and the number of verified nodes is recommended to be no less than 6 nodes.

## Consensus algorithm

The SWTC Public Chain technology uses a self-owned proprietary BFT consensus algorithm.

under PBFT mechanism, there is a concept called view. in a view, there will be primary node (replica), and the rest of the nodes are called backups. The primary node is responsible for ordering the requests from the client and then sending them to the backup nodes in order. This primary node of PBFT has more rights than other nodes, and if it has a problem, it will cause a relatively large delay in the system. in rBFT, this point has been improved. referring to the mechanism of election in raFT, voting is adopted, and there is no need to snatch the accounting right to ensure the fairness of the rights of each node.

## Financial blockchain

The financial blockchain is an alliance chain and a permission chain.

The financial blockchain is a network of companies in the financial industry. Through this network, various financial services are run. Only transaction members in the alliance are eligible to view it. Therefore, members of the alliance need to be approved to access the alliance chain. .

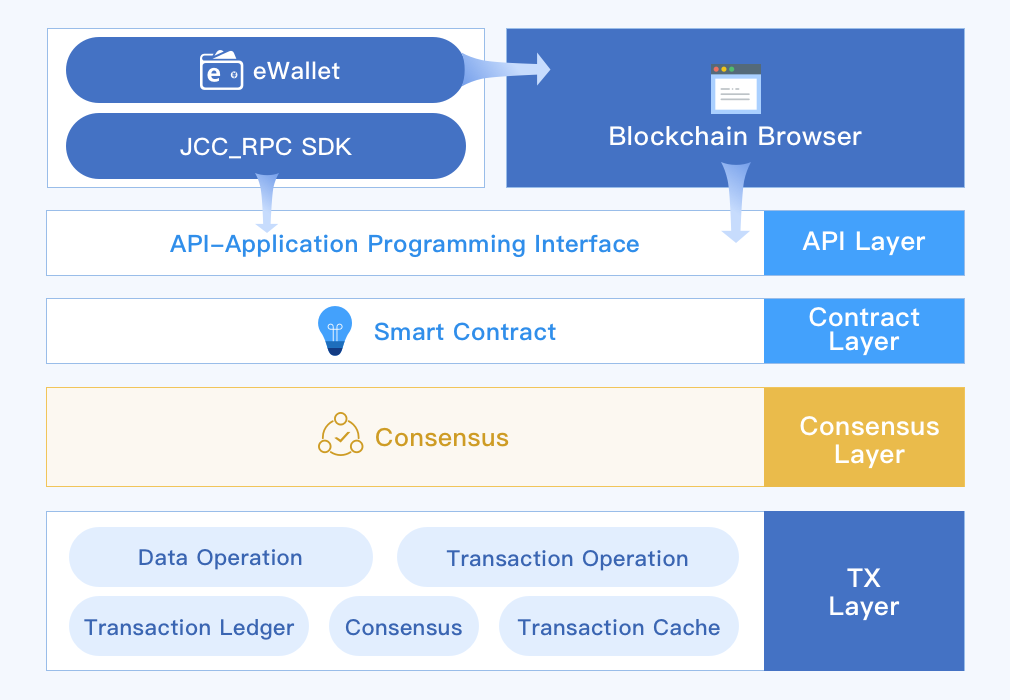
The regulatory authority (including the tax authority of the host country), as one of the node members, monitors transactions in real time to meet anti-money laundering regulations and other business regulatory requirements. In the event of a violation of the regulation, the relevant transaction wallet can be implemented through the alliance chain’s governance mechanism. Freezing to prevent greater illegal consequences.

# Software architecture

The actual combination of blockchain and financial services is different from traditional centralized systems in terms of software architecture. This chapter not only explains through the architecture, but also explains the application in different scenarios.

## Overview

The software architecture of financial applications is as follows:

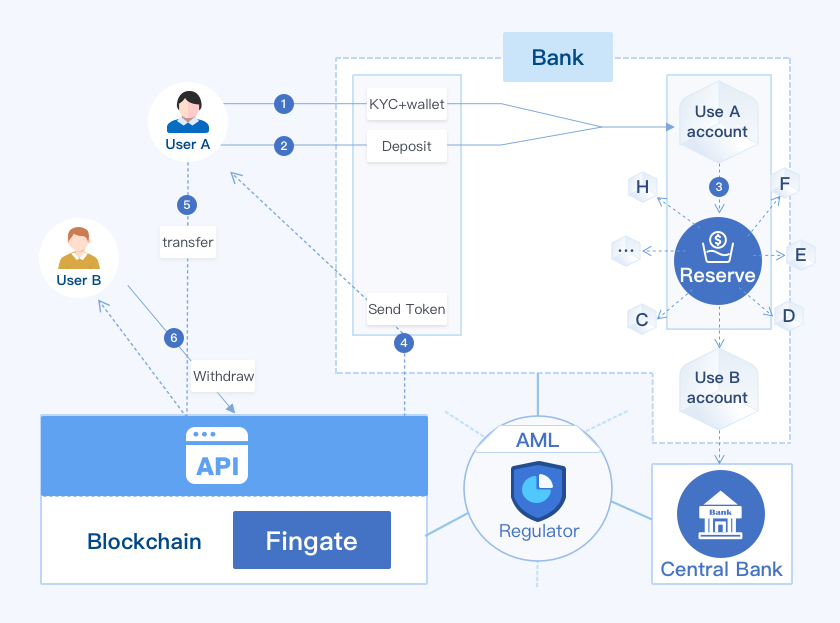


As an application, for example (eWallet), the ability to access blockchain services is obtained by integrating the SDK. In the area below the API, it can be regarded as a blockchain node service. There are many such nodes in the entire blockchain network. Applications can choose any node and can run.

The design of the blockchain is based on the credible purpose of the ledger. Therefore, the blockchain API is inefficient for statistical classification and query of transactions. Usually, this responsibility is performed by the browser service.

## Payment

As a bank, to use the blockchain for payment, you need to map the real funds and the tokens circulating on the blockchain. The business framework is as follows:

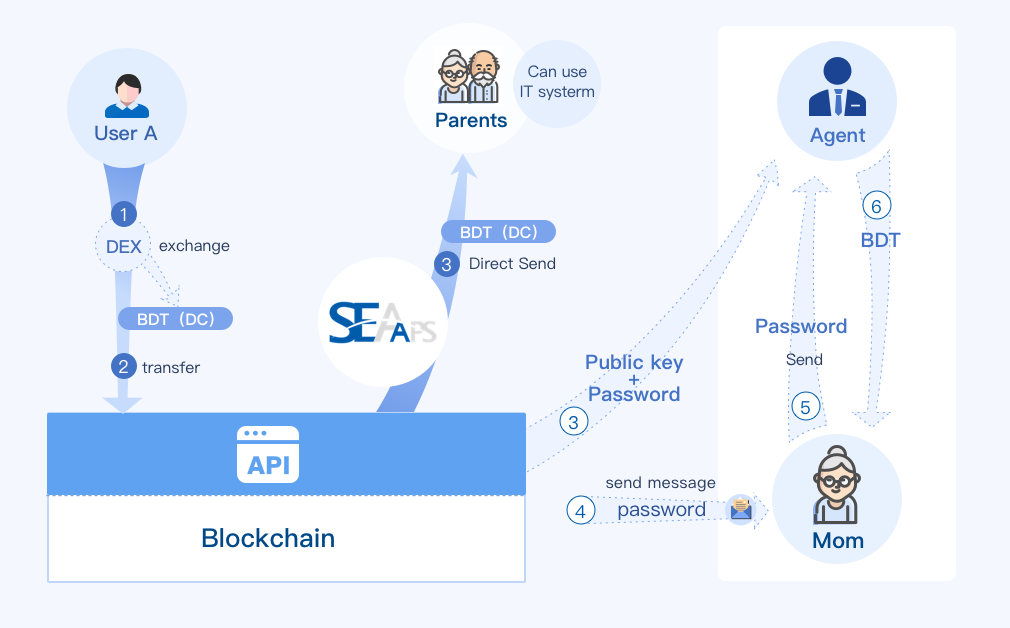


1. The user (company) registers the blockchain wallet, completes KYC at the bank, and binds the user with the bank account;
2. The user (company) deposits currency to the bank;
3. After receiving the currency, the bank transfers the corresponding funds from the user’s bank account to an escrow fund pool account;
4. The bank then transfers the digital currency to the user’s wallet;
5. Users can pay digital currency directly to user B’s wallet;
6. If user B needs to withdraw cash into his bank account, he just transfers it out of the blockchain wallet to his bank account(Fingate);
7. After the bank detects the change of funds, according to the transaction request, it transfers the funds in the fund pool to the bank account of user B;
8. Regulatory nodes supervises payment activities on the blockchain to meet anti-money laundering (AML) regulatory requirements. Each wallet is KYC-made.

The funds in the capital pool(Reserve) in the figure are the sum of the asset tokens circulating on the blockchain, and the amounts on both sides are exactly the same.

## Remittance

For the remittance, the blockchain-based process is as follows:



For users who will use mobile APP, after receiving the token, they can use the APP to pay directly, or withdraw the funds to their bank account through the bank’s fingate.

For users without a bank account, the sender can use double encryption to send money.

1. The sender transfers the token to the withdrawal point wallet closest to the recipient, and the note is double encrypted with the withdrawal point wallet address and the password specified by the sender;
2. The sender informs the recipient of the password via other way such as SMS, phone;
3. The recipient goes to the withdrawal point and tells the password. The withdrawal point uses the wallet private key that only he knows and password to decrypt it, and obtains the note information. After verifying the recipient’s identity, the payment is made;