Anlink Blockchain Network

Whitepaper

V 1.0

Jan-2017

ZhongAn Tech.

1 Abstract

Blockchain[1-3] is a distributed open ledger which is shared and maintained by all the nodes in the blockchain network. In retrospect, from the earliest “born for currency”, blockchain has already developed into a “revolutionist” in different industries like credit service, bank, insurance, security,etc.

With years of research and build-up in blockchain technology, we believe that blockchain’s value shall definitely not be limited to digital currency in the future. To advance blockchain with more value in commerce adoption and vitalize traditional industries is our mission to develop new blockchain products.

This paper introduces Anlink network, which is a blockchain cloud network composed by Ann-Router and AnnChain together with other blockchain systems.

Ann-Router empowers blockchain to connect and communicate cross chains. By establishing a cross blockchain communication protocol (CBCP), Ann-Router makes it possible that different blockchains in the network can communicate with each other same like other equipment in the internet network. In the network of Ann-Router, some blockchain plays the role of a router which, according to the communication protocol, analyze and transmit communication requests, dynamically maintaining the topology structure of the blockchain network.

To make the blockchain system meet the requirements in regulation, privacy and complicated commercial adoption, we design the Anlink, an enterprise-level blockchain product. This paper explains its architecture, characteristics, advantages and application in detail.

2 Introduction

Blockchain’s commercial value has got the best proof through the blockchain projects of Bitcoin[4], Ethereum[5],etc,. Digital Currency is accepted by users for its advantage in decentralization, immutability, etc,. At the moment, many blockchain projects focusing on digital currency has developed into mature and stable ecosystems. However, due to blockchain’s long-time isolation from the outside world, the existing blockchain ecosystems become isolated islands. Except few blockchain projects like BTCRelay who has done some exploration in the cross-chain interaction, digital Currency Exchanges are still the most common means to transmit digital asset cross chains. These Digital Currency Exchanges uses blockchain as gold mines with traditional operational management, trading digital currency as cargo, which can only create limited values.

Reviewing Internet’s development history and the changes it brings, we can not deny the

tremendous power of telecommunication. In fact, the birth of the blockchain itself is a prospective product of Internet. Without relying on centralized service, the blockchain nodes establish mutual trust through P2P communication, consensus, back-up data. Developed so far, Internet encounters many problems, such as, the increasing load of backbone network and fthe request attacks, and is seeking for solutions actively. For example, IPFS[6], the content-based distributed network file storage protocol, can deal with the problems faced by the traditional IP address based network protocol.

By analogy to Internet, it is not difficult to find that, in the current phase, blockchain's network capacity is only carried out to the extent similar to LAN, and different chains cannot communicate and has no mutual trust at all. For a single blockchain, we also suffer from its various limitations. Meanwhile, the consensus mechanism, in providing security, also greatly limits the development of blockchain system at the same time, which leaves us no way of improving the processing capacity of the transaction by increasing the nodes. If blockchain is to embrace a brighter future, these issues must be addressed.

In the context of commercial applications, enterprise blockchain products, from both its technical characteristics and service groups, are different from the public blockchain represented by Bitcoin, Ethereum, etc,.The primary requirement of enterprise blockchain products is to meet the requirements of regulation and privacy protection, as well as supporting heavy transaction load, data sharing, and preventing the "Byzantine Generals Problem".

This paper is organized as follows. The third chapter introduces the design concept of the Ann-Router system, including design inspiration and vision. The fourth chapter explains architecture of the Ann-Router. The fifth chapter explains the cross chain communication protocol. The sixth chapter gives the design of AnnChain, the sub-chain to address complex business requirements. The seventh chapter looks into the future of the Ann-Router and AnnChain's commercial application.

3 Design Concept

In the face of various problems in blockchain's development, we put forward the concept of "Ann-Router". It has two main purposes, firstly, Ann-Router shall empower the blockchain system's processing capacity of transactions as well as its scalability; secondly, Ann-Router shall break down the communication barriers across chains, realizing connection, communication, trust cross chains.

3.1 Design Inspiration

The design concept of Ann-Router is derived from the routing architecture of the Internet. A simple routing network consists of routers and terminal devices. The terminal device has a unique IP address, the router maintains a routing table that reflects the address it can jump to,

and the routing table of all routers constitutes the topology of the entire network.

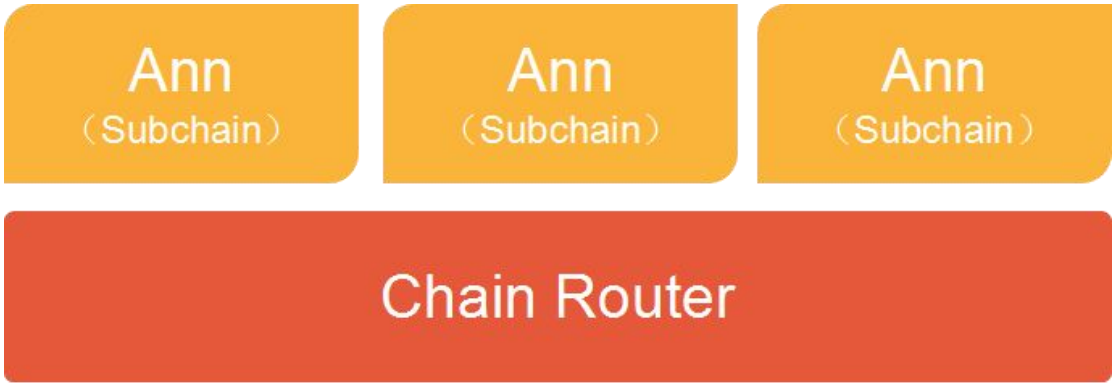
The blockchain systems, such as bitcoin, Ethereum, AnChain,etc, corresponds to the terminal equipment in the routing network, which is called “sub-chain”. A sub-chain can receive messages from a chain router, or send messages to another sub-chain via the chain router, but cannot communicate directly with each other.

Besides offchain channels, we design the “Ann-Router” same as the router in Internet. Ann-Router dynamically maintains all the related information registered on sub chains , which is used to link sub-chains in the blockchain network. To communicate with other sub-chains, a sub chain must firstly establish connection with Ann-Router through cross chain communication protocol. Ann-Router can communicate with a sub chain or other Ann-Routers. By exchanging information with its connected sub-chains, Ann-Router maintains the smoothness of the network communication.

3.2 Vision

In this structure, we can deploy blockchain network system according to different business logic and user requirements.

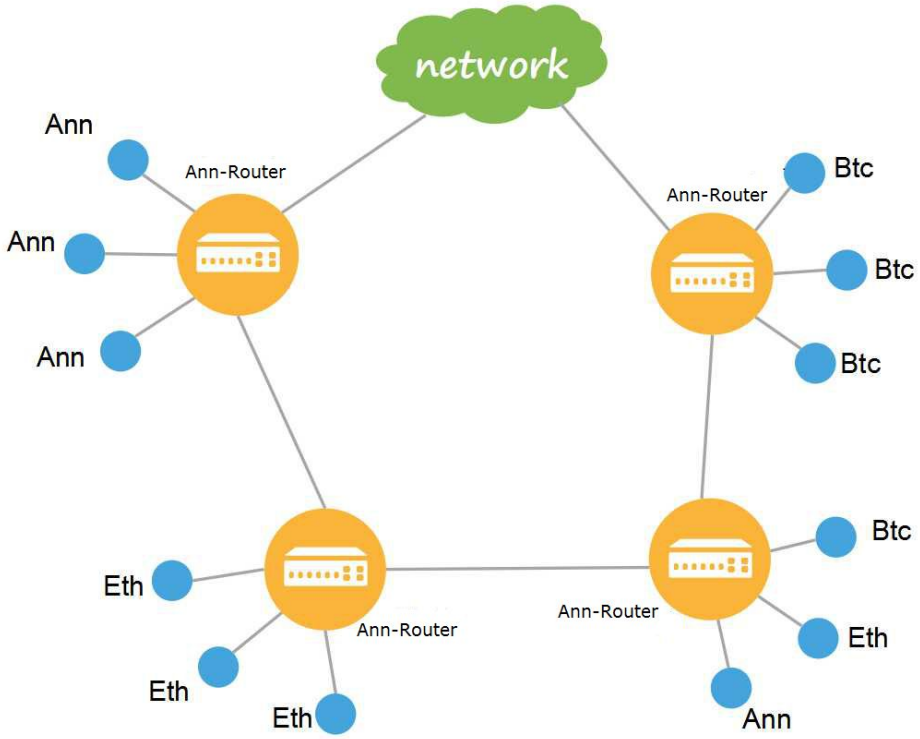
We realize sharding of the blockchain by Ann-Router and improve the transaction processing capacity of transaction on the blockchain system. Compared with single blockchain system, the Ann-Router system can grow linearly in its transaction processing capacity by connecting multiple sub-chains. The request of transaction can be assigned to different sub-chains through Ann-Router, which can effectively avoid centralized requests on a sub-chain. In addition, we can deploy clusters of isomorphic sub-chains with different volume on Ann-Router. For isomorphic sub-chains, the cluster with more nodes is more secure, while the cluster with less nodes shall have faster processing speed. The blockchain sharding by Ann-Router can empower the chain network with flexible deployment according to business requirements.



Of course, besides the realization of blockchain’s sharding, another important significance of the

Ann-Router is to break down the communication barrier among sub-chains , and establish trust bridge cross chains. The sub-chains connected to Ann-Router can communicate information with each other and work together to achieve the effect of "1+1>2". We can also deploy a number of Ann-Router systems, each chain can be deployed in the routing system, with isomerism sub-chains including Bitcoin, Ethereum, AnnChain. Thus, each Ann-Router can serve a more complete business ecosystem. Similarly, we can deploy different Ann-Router clusters according to nodes numbers, geographical location, business requirements. Following the Routing algorithm, different processing requests shall be assigned to appropriate cluster.

The final form of the Ann-Router network is the formation of complex block chain star network, which is connected to each other by the infinite extension of the Ann-Router and interconnection, creating a blockchain network which is interconnected and communicable with trust.



4 Ann-Router

In the Ann-Router network, some sub-chains, such as bitcoin, Ethereum, etc, are prior to the existence of the Ann-Router, and at the time of these sub chains designation, these sub-chains did not have the function of cross chains communication. While Ann-Router can be accessed by every sub-chains same as internet router's logics, thus we put forward a set of designation on Ann-Router and cross chain communication protocols, and the blockchain systems conforming to these protocols can connect to Ann-Router easily. For those early blockchain systems, without changing its designation, an extra adaptation system is needed to assist its communication with Ann-Router. In this section, we will give a detailed introduction to Ann-Router.

4.1 Consensus Algorithm

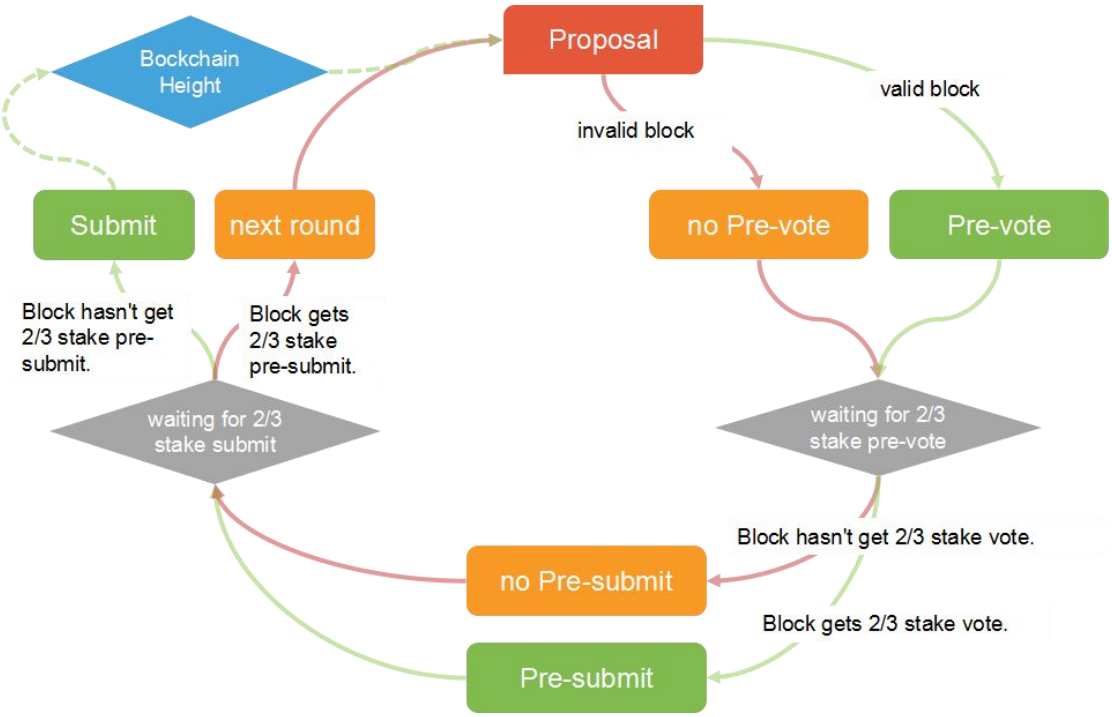
Proof of Work (PoW) is a Byzantine Fault Tolerant (BFT) consensus algorithm that is applied to bitcoin and ethereum. Since the launch of bitcoin, PoW has proved its reliability, but the waste of resources is also obvious. Proof of Stake (PoS) is an alternative consensus algorithm aiming to solve the resources waste in PoW. However, there is still big differences between PoW and PoS, and the most important difference is that the computing power in PoW can not be distributed. A miner with fixed computing power can not mine on two chains at the same time as well as doubling the total computing power. But the voters with stakes can vote to every possible blockchain, and could get guaranteed of their interest as long as any of their voted block wins in the game. But there is also great security risk, as it greatly reduces the evil doers' evil cost.

Raft is a common and effective consensus algorithms, but its biggest drawback is that it cannot prevent Byzantine nodes and a Byzantine leader node with powerful network configuration shall give Raft consensus devastating blow. In the development of Byzantine fault-tolerant consensus algorithm, some algorithms combining Raft and BFT are proposed. Take PBFT used by AnChain for example, some reliable nodes are called validators who have the chance to become leaders. In the process of blockchain generation, a new validator shall become this round's leader in default, and this leader is responsible to package the new block and broadcasts the reasonable block to every validator. Only after two rounds of more than2/3 commit among all the validators, can the new block be confirmed in consensus. This consensus approach greatly improves the speed of the block generation, and as long as less than 1/3 validators are not Byzantine nodes, the block can be generated continuously.

Undeniably, the Byzantine fault tolerant algorithm used in PBFT can guarantee the network security whose Byzantine nodes is less than 1/3. However, in practical application, especially when associated with economic benefits, even if the validator is reliable nodes selected, we can not simply rely on the 1/3 security without punishment mechanism. To ensure security, there must be immediate reward with persuasion and immediate penalty with punishment, also the reward and penalty must be associated with economic interests. Therefore, we modified the original consensus mechanism, to make the validators' voting rights correspond to the token they mortgaged on the chain.

In this way, the blockchain generation mechanism is changed to over 2/3 commit stakes' confirmation from over 2/3 validators. Besides, in PBFT consensus algorithm, the common nodes only synchronize the new block information from leader's nodes without taking part in the consensus. Its security only rely on the validation nodes, thus the increasing in common nodes number can not improve Byzantine fault tolerant's security. In our new consensus mechanism, we increased the non-validator nodes' involvement. A validation node shall be bonded with a validator account, and the non-validators can delegate their stakes to validators while winning benefits. In consideration of their benefit interests, the non-validators shall choose their authorized validator with great care. This consensus mechanism ensures all nodes get involved in the consensus while reducing the low efficiency problem.

This consensus algorithm is called Delegated Stake-PBFT, referred to as DS-PBFT.



4.1.1 Light Client Terminal

Common blockchain client terminal requires to synchronize all the blocks on the blockchain to verify a transaction. Powerful as it is, it is still heavy loaded with too much backed up data which brings much inconvenience in actual application. By using DS-PBFT consensus with validation commit, Ann-Router enables the light client terminal for users.

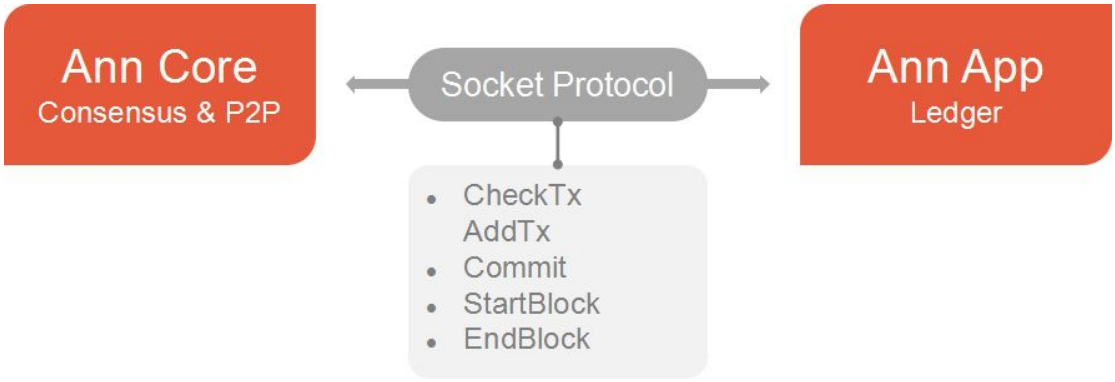
For verification of information, the Light Client Terminal only need to synchronize the newest validation set on the blockchain time to time. The Light Client Terminal can trace and verify the updated block height, global status, etc. by continuously synchronize the block head and validator's information. Of course, compared to the client terminal with complete nodes

validation, Light Client Terminal can realize limited functions, while it is more suitable to mobile terminal and IoT equipment without big hard drive storage space to get important status data.

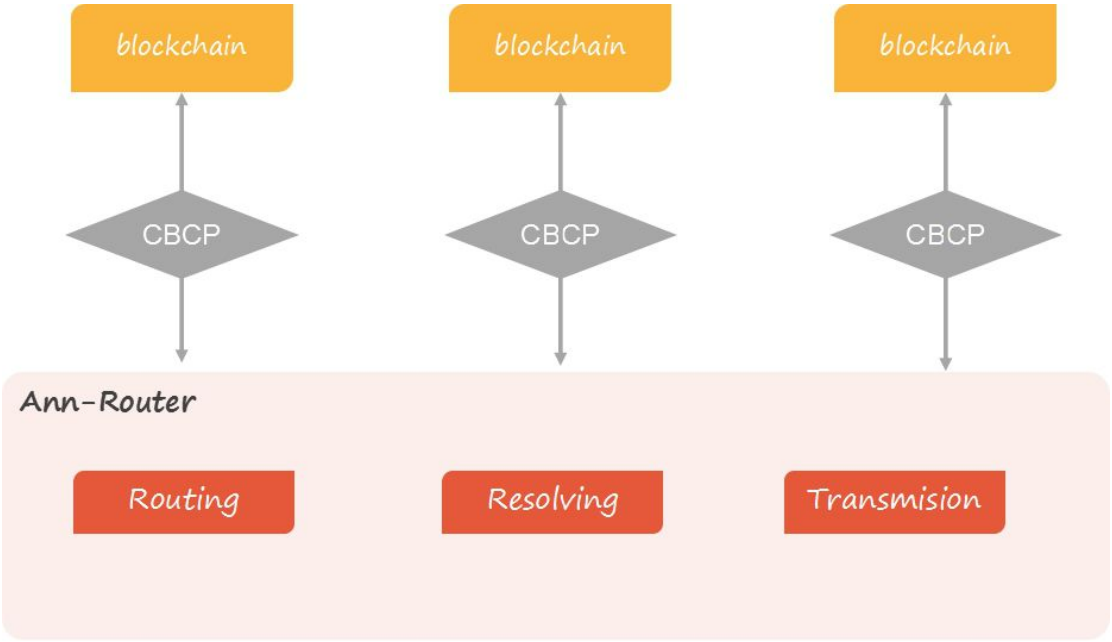
4.2 Architecture Analysis

4.2.1 Ann-Router

Different from traditional blockchain system, consensus algorithm and P2P network in Ann-Router is closely related with ledger logic, which divides Ann-Router into two parts. Consensus algorithm along with P2P network is called AnnCore which is responsible for transaction broadcast and consensus. While the ledger part is called AnnApp which is in charge of verification, inquiry,etc. AnnCore and AnnApp are connected by socket protocol. Thus, AnnCore can replace the consensus and P2P network in many traditional blockchain systems.



Acting as a router in the blockchain network, Ann-Router can analyze communication data package with communication packet processor, and send messages to sub-chain through Cross Blockchain Communication Protocol according to the Routing table dynamically maintained by itself.

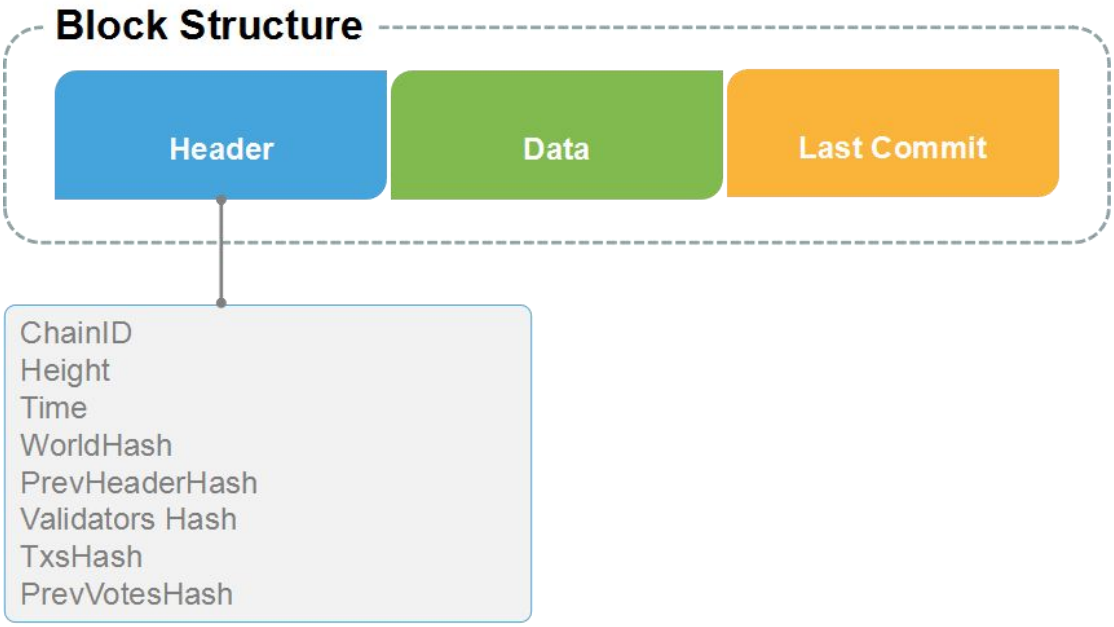


4.2.2 **Block**

Since Ann-Router adopts DS-PBFT consensus, its block architecture is strongly different from that of Bitcoin and Ethereum. From the structural perspective, Ann-Router's block is composed by three parts: Header, Data, and Commit.

The Header includes: chainID, block height, time, hash value of the global status, hash value of the previous block header, hash value of the shards, hash value of validators, hash value of the Data, hash value of the commit, etc. The last two of the above mentioned are the integrity validation of the block. The block data contains all the transaction data in this block. The commit is designed to establish connection between this block and the previous one.

As mentioned before, only through two rounds of more than 2/3 stake vote can consensus be achieved, in which the second round's commit will be recorded. When the new block is proposed, the last commit will be included in the new block's voting process. Thus, voting on the new block will always contain the last commit on the previous generated block.



4.2.3 **Layered Structure**

In ideal condition, Ann-Router itself serves as one single blockchain, through which all the sub-chains can communicate with each other. The advantage of this design is the high speed of communication. However, with the increase of sub-chains, total communication processing load shall rise and consequently the storage and computing load of Ann-Router will be dramatically increased. Thus layered structure is introduced.

To simplify the problem, we hypothetically assume that there are two layers in Ann-Router: The bottom chain is to connect with the upper chain as well as maintaining cross chain communication among upper chains. If target chains are on the same upper chain layer, communication can be carried out on the upper layer. If target chains are separated in different chain layers, then bottom layer chains come into play for the communication. In real use cases, Ann-Router may have more than two layers, with the bottom layer acting as the Router's backbone supporting the whole network structure.

The problem of layered structure is communication delay and storage redundancy. In general case, if messages need to be transmitted through multiply layers of Ann-Routers, it will cause a time delay and increase Ann-Router's storage burden. In the case, we need to optimize the routing algorithm, which can facilitate the optimization of the routing path within short time and be adaptive to multiple unpredictable network environment rapidly and precisely. The routing algorithm uses multiple measurements to select the best path. Through weighted operation, Ann-Router combines the measurements into single compounded measurement and sends it to the routing table as path searching standard. The measurement includes network time delay, work load, and communication cost.

4.3 State Maintenance

As communication bridge between different blockchains, AnnRouter is responsible for some state maintenance of the sub-chains.

First of all, sub-chain must register on AnnRouter before communicating with it. The registration includes ChainID, the validator information on the chain, the assets information on the chain, etc. Through this can the Ann-Router identify the specified sub-chain on the communication request and complete the transmission operation.

Then, AnnRouter need to synchronize sub-chain's updated block information and commit data of the latest block. By doing this, Ann-Router is able to maintain sub-chain's basis state, assisting users of the light client terminal to search for sub-chain's height and status, and validate transactions sending from sub-chains, etc.

Moreover, as validator's identity is changing time to time, Ann-Router need to maintain the validators' information on every sub-chains, which is necessary for the transaction validation.

In like manner, it's also necessary for sub-chain to maintain information on Ann-Router. By doing this can the transaction be confirmed to be send from the Ann-Router. The information includes Ann-Router ID, validator information on Ann-Router, lasted block and commit on Ann-Router, etc.

4.4 Auto Scaling

One important breakthrough of Ann-Router is to enable the blockchain system with Auto Scaling. Before Ann-Router's transaction capacity reaching to its limit, new sub-chain can be added to the network to reduce the transaction load on the current sub-chains. To make the newly added sub-chains on the Ann-Router taking over the pressure rapidly, a real-time response routing algorithm is designed.

Ann-Router maintains a list of the sub-chains registered on it. This list will be updated beforehand if any sub-chain need access to the network. The light client terminal will read the latest sub-chain's number on the parental chain time from time that emulates a distributed configuration management mechanism. The light client terminal will randomly pick a timeout value between 0.5 and 1 second and countdown its clock. When time is out, the light client sends a query of sub-chain amount to the Ann-Router and stored the response data in local files. If the inquired result is different from that stored in the local file, the client terminal will broadcast the latest data with time stamp to the other light client terminals. The client receiving this data will also compare it with its own copy. If it is same as its local copy, the clock is reset and a new timeout value is set. Otherwise, if it is different and the time stamp is later than the local data, this client will send an inquiry to Ann-Router and reset the clock when new data is updated. While if the receiving data is different but the time stamp is earlier than the local written time, this data can be ignored. Moreover, a shielding mechanism is designed to block suspected

dishonest client. When a broadcasting data received from that client is proved to be wrong, receiver can choose to block that client in a short duration of time. But wrong data can not prove the sender is a liar, because the sub-chain amount could be changed in a slice time gap and cause the honest data to be wrong later. The light client terminal can choose to block the cheater's message, and the block time duration will increase as the dishonest incidents happens more frequently.

The above method ensures that the data stored on sub-chains in the light client terminal and Ann-Router are synchronized time to time. As a transaction request is initiated from the light client terminal, the light client terminal shall appoint a trigger chain. By calculating the hash value of the application identification and the sub-chains' number stored at the local files, the result is the target chain's serial number as requested.

4.5 Ann-Router Management

From the management perspective, Ann-Router and Anlink are independent from each other. Ann-Router will not affect the performance of Anlink, and vise visa. This part explains the management rules of Ann-Router.

4.5.1 Validator Management

Validator is crucial for the normal operation of the Ann-Router. At the time of Ann-Router's initialization, some nodes will be appointed as the first batch of validators. With the increase of the nodes number, the validators will increase by same percentage until the number reaches the maximum. New validator will not be added to the network if the maximum number is reached. But to ensure safety and liquidity, a validator removal mechanism is introduced. For those corrupted validator, a removal proposal can be initiated for commit to decide whether or not that validator should stay or not.

The allocation mechanism is as below. At the first year, the maximal number of validators in Ann-Router system is 200, and shall increase linearly by the annual growth rate of 10%. Then the second year will have 220 validators, the third year 242, the fourth year 267, etc. In the case that the maximal validator number can not meet the network requirement, a proposal of adjusting the maximal number can be submitted.

4.5.2 Token

Ann-Router issues its own token ZAC through Proof-of-Stake (PoS). In the initial stage, a crowd funding is launched before Ann-Router's initiation. The total amount of ZAC is divided among the crowd funding investors, Zhongan Tech., and Shanghai Blockchain Industry Alliance by the corresponding percentage of 35%, 10% and 35%. At the initial stage, ZAC will be paid back to investors daily according to his investment, i.e., the investor can receive 1/365 of his total ZAC value every day. The issuance of ZAC is in inflation mode, and the annual inflation rate is 10%.

Every two weeks new ZAC will be generated and paid to validator nodes as the rewards of their contribution to the network maintenance. The reward ZAC is allocated among validators according to their investment of ZAC for their involvement in the ledger stake. ZAC can be used to pay for transaction fee charged in Ann-Router system. This mechanism can efficiently avoid DDoS attack against the network, and the transaction fee will also be distributed as rewards among validators.

4.5.3 Stake Management

Every ZAC owner has the chance to become a validator by mortgaging his ZAC to a shared ZAC fund. The commit weight of each validator is decided by the portion of his ZAC in the fund. Before the number of validators reached the maximum, every ZAC owner can apply for the position of validator. When the maximum is reached, one owner must mortgage more ZAC than the least owner of current validator to take the validator position. Those nodes who does not have enough ZAC can delegate his stake to a node of validator, and the reward to this validator should be further allocated to its consignors. In this way, the nodes having few ZAC can also contribute to the network consensus and avoid economic loss caused by annual inflation.

4.5.4 Reward and Punishment

Validator can raise a proposal which can get approval as more than 2/3 total stake commit reach a consensus. There are 5 types of commit, including agreement, intensive agreement, disagreement, intensive disagreement, and abstention. If over 1/3 total stake commits intensive disagreement, the proposal will be rejected and the validators who commit agreement and intensive disagreement will be punished. As the result, the validators' ZAC in the fund will be reduced and the same amount of ZAC will be added to the reward pool. Those proposals approved will be executed in two weeks.

The design of reward pool is a kind of encouragement. For example, the bug founder could choose to submit the bug statement by ReportBugTx and his reward address to the network. And if the proposal of this bug report is approved, the network would reward him by using the ZAC in the reward pool.

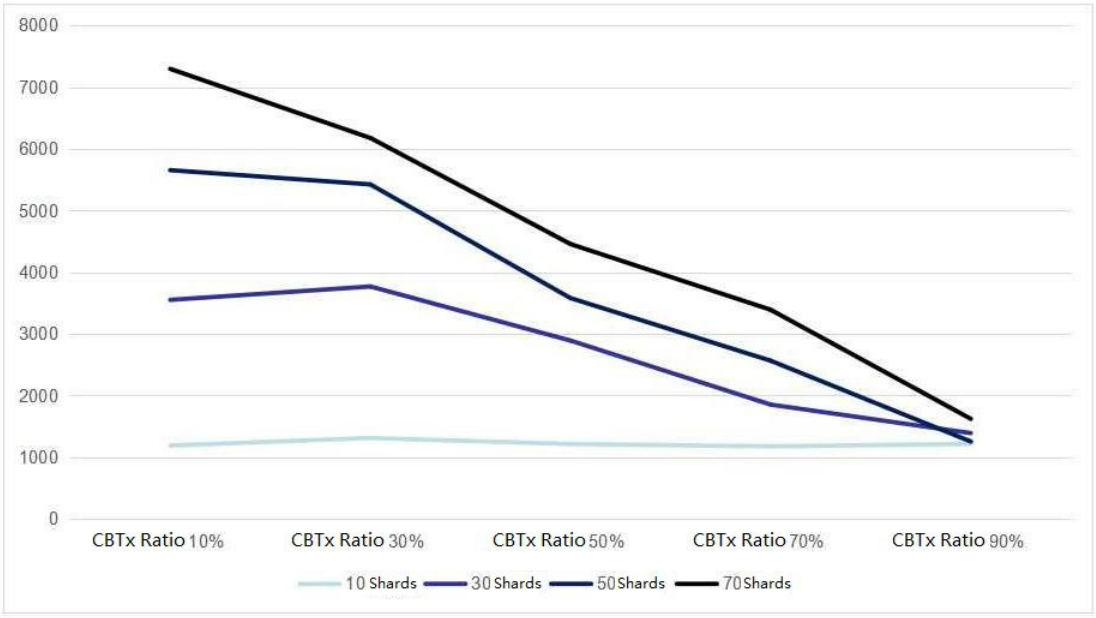
As a crypto-currency, ZAC can be traded on exchange platform just like Bitcoin or Ethereum. So, people could trade ZAC for speculation. When ZAC price is suddenly increased, the revenue of running a validation node turns out to be less than directly trading ZAC in the market, which will cause the validators to draw back their ZAC mortgage and stop being a validation node. In order to ensure the safety of Ann-Router, when the number of validator is in the range between 30%~50% of its maximum, the reward of generating new block will be one and a half time of normal reward. And when the number of validators is lower than 30% of its maximum, the reward becomes 2 times. In extreme cases, all the nodes can submit a proposal to adjust this reward ratio.

A validator could make a negative influence to the Ann-Router system intentionally or unintentionally, thus a punishment mechanism must be introduced into the DS-PBFT consensus algorithm. Double-signing and abstain are two typical cases need to be punished. Double-signing means the validator signs on two different blocks for the same block height in the same commit round. Such action will affect the DS-PBFT algorithm. Once double-signing is found, some ZAC will be deducted from the validator and its reputation will be damaged also. If the reputation of some validator is negative, it will be removed from the validator list. Validator may go offline for a long time because of network failure or machine damage and consequently be absent from commit. Even in this case, if the validator is absent too often and the absence outnumbers the validator Max Timeout, the validator shall also be punished.

The above violation can be easily detected. But for those violations not easy to find out, a two-week unbundling process is required for ZAC so as to extend the time of violation detection.

5 Performance of Ann-Router

In lab environment, tests show that Ann-Router's total transaction processing capacity is growing linearly with the increase of sub-chains. The performance of a single Ann-Chain varies between 20tps to 180tps due to the complexity of the transaction. By running tests on the scaling capacity of Ann-Chain equipped with Ann-Router, we get the Ann-Router System's transaction capacity variation data under different shard numbers and cross chain transaction ratios.



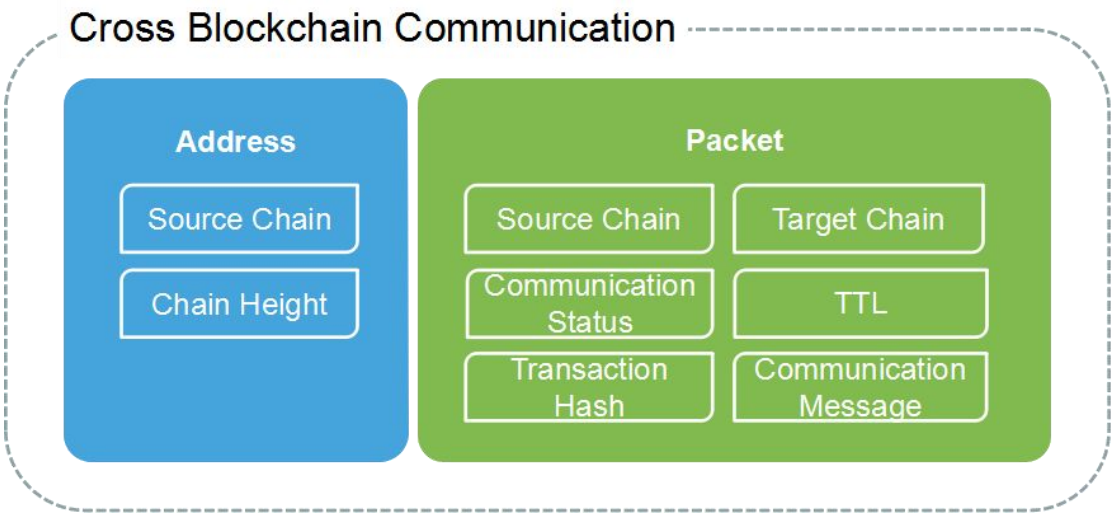
6 Cross Blockchain Communication Protocol (CBCP)

The communication protocol cross blockchains is similar with that of TCP / IP in traditional networks, and the message, including Header and Data, is delivered by establishing a reliable connection cross blockchains. Header records the message's source, destination, length, and classification, etc. In the transmission process, the Header will be stripped off layer by layer, modified, and message shall be transmitted to the destination. In addition, message's transmission will have responding status, and the sender can give appropriate response according to the receiver's feedback on the current communication status.

6.1 Protocol Structure

A complete Cross Blockchain Communication Protocol consists of two parts, communication address and communication packet.

The communication address includes source ChianID and Height of the message source chain. Communication packet is composed of header and data. The header includes source ChainID, target ChainID, status, TTL, and communication transaction, etc. The communication message will not be opened during the transmission.



Communication status corresponds to the communication status mechanism in the Internet communication protocol. When a communication packet is transmitted, the communication status is "pending". When the receiver receives the message, it will send back a packet whose communication status is "transmitted", if the sender got the packet with "transmitted", the sender will respond with a packet of "received". The above process is complete a success communication. In the process, if the receiving of packet fails, the receiver is not responding with "transmitted", the sender shall resend message sometime later, trying to rebuild communication.

Besides the above mentioned status, we also specify the "connection timeout" status. When a

transaction is sent from sub-chain 1 to sub-chain 2, the communication survival time decided by Ann-Router's block height is indicated. The Ann-Router will send communication status to sub-chain before reaching the communication survival time. If the communication surviving time is exceeded, the Ann-Router will send "connection timeout" status directly to the sender. The sender's sub-chain records this communication as a communication failure.

6.2 Communication Verification

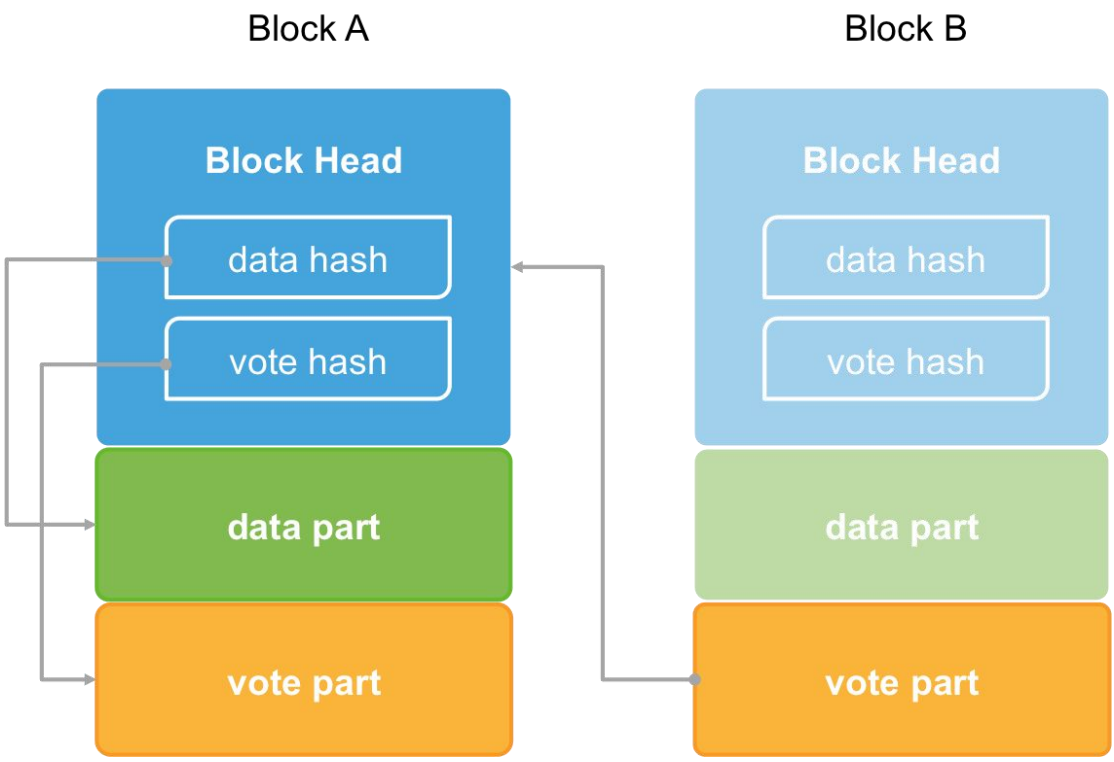
Similar to network communication, cross blockchain communication may also be attacked, especially DDoS attacks. Therefore, we need a set of verification mechanisms that are user friendly and anti-counterfeit, preventing the Ann-Router from being paralyzed due to attacks.

The Ann-Router Architecture referred in Chapter 4 is a standard framework we believe that sub-chain should have. In the standard framework, the Ann-Router can verify communication request sent by sub-chain easily. As mentioned above, sub-chain sends the latest block and commit to Chain-Router from time to time. As a transation is transmitted, the blockchain height of the Exchange will be reflected in the communication address. We only need to look into the blockchain height if this transaction exists or not, as the submission of the lasted block and its commit can already prove a block's authenticity, referring to below listed logic:

First of all, a block alone can not prove its legitimacy. Because for an existing block, we can forge an illegal false block but consistent with the block architecture, i.e., modifying the transaction of the block Data and the transaction hash value in the Header.

As mentioned above, a block is proposed for consensus after two rounds of voting, in which the second round of the consensus commit will be temporarily stored, which serve as the connection part of the previous block to the new generated block in the next round. Based on this, if sub-chain submits some block and its voting at one time, we can verify this block's honesty within the block generation time. We don't have to waste two block generation time by waiting for the next block to generate and prove the previous generated block's reliability by verifying the following connected block's validation information for it.

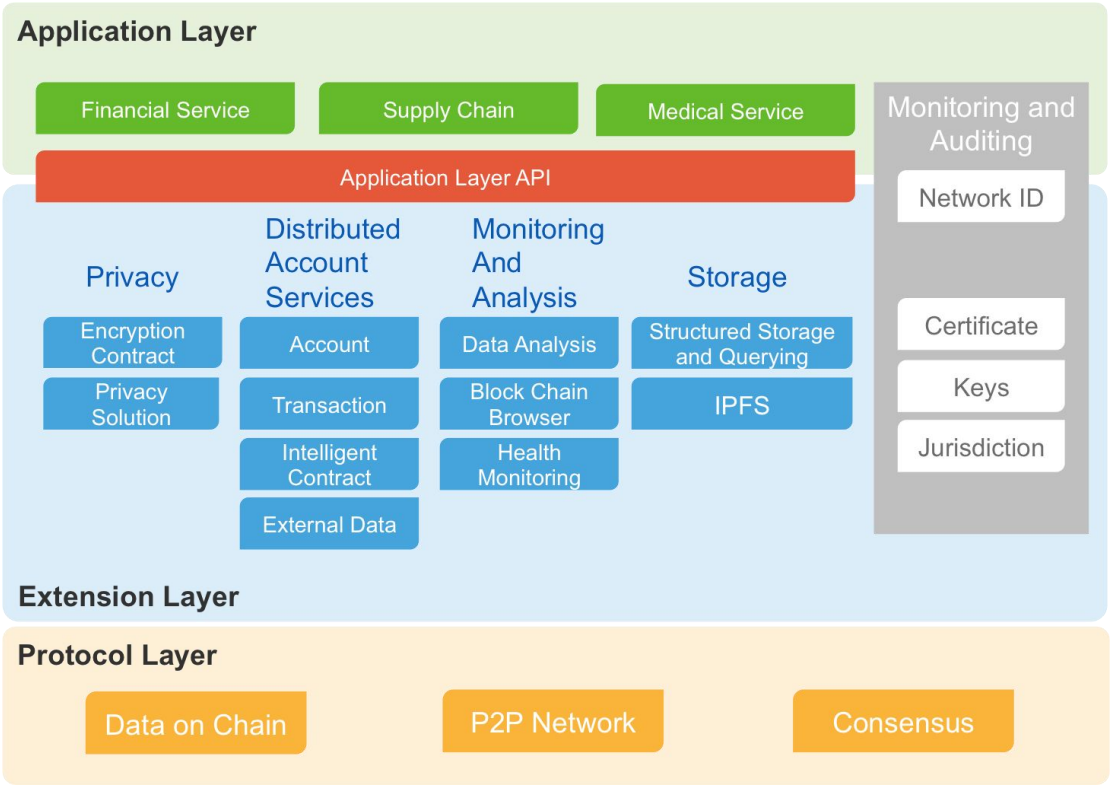
The process of validating the legitimacy of an independent block by consensus is to verify that the block, except the Header, has not been tampered with, by checking the block Data in the block Header and the hash value of the voting. Plus, the commit is the cluster of digital signatures of more than 2/3 validators on the block header. Unless the message sender controls private keys of more than 2/3 validators of the blockchain, he cannot counterfeit the block.



7 Ann-Chain

At the beginning of the design of Ann-Chain, we have already schemed it as an enterprise-class blockchain product. Ann-Chain's design objective is to meet various requirements of commercial applications, including the establishment of a practical audit mechanism; transaction privacy protection; stable, efficiency and reliability; establishment of a platform for data sharing.

The diagram below shows the architecture that the Ann-Chain refers to, which is a logical structure but not the physical description of specific procedure, address space, or equipment components. In order to absolve the possible obstacles in blockchain's application process, Ann-Chain is designed with a three-tier architecture: (1) protocol layer: to provide basic services of immutable storage and synchronization of the original data on blockchain base layer. (2) extension layer: to realize various functions of Ann-Chain, including monitor, privacy, smart contract[8], monitoring analysis, structured data storage and inquiry. (3) application layer: to run various applications on Ann-Chain, such as banking, medical,etc.



The main function of the Ann-Chain is implemented in the extension layer, the main modules are listed as follows:

● Supervision and Audit Module: to provide trading authorization and supervision on chains with certificate issuance and authorization management.

● Privacy Module: to provide encrypted contract transactions and privacy solutions for different scenarios, such as multi-party computing [9], PGP communication and ring signature.

● Distributed Ledger Services: to provide interpretation and execution of transactions and smart contracts, transaction management, and external data services.

● Monitor and Analysis: to support monitoring for system and hardware environment with multiply visual management tools to meet the management and maintenance requirements.

● Storage: to provide file storage, structured data storage and inquiry.

The protocol layer stores the raw data on the block chain and synchronizes the global status among nodes. The protocol layer consists of three parts: the data on chain, P2P network and Consensus Manager.

● Data on-chain: The data on the Ann-Chain are represented by transactions, and each transaction contains a signature. Transactions are packaged in blocks, and adjacent blocks are linked by a hash chain. The Ann-Chain uses status model with every transaction changing the blockchain status. The explanation of status changes caused by transactions is provided by the upper ledger service.

● P2P network: Blockchain network is a multi centralized nodes network, and message publish and transmission between nodes adopts P2P module. In P2P network, each node can attain service from other nodes, as well as provide message service to other nodes. The P2P protocol of

Ann-Chain adopt authorized and encrypted security communication mechanism.

● Consensus: AnnChain's consensus algorithm is based on PBFT. The blocks generated by the algorithm are through voting, and the block generation time is stable, while the block generation time based on PoW consensus is decided by probability. In the algorithm, the transaction block which is confirmed on the blockchain is recognized as the final status, and neither the blockchain will fork nor has genomic block which can enhance the throughput. The algorithm can resist the node's error messages and collusion with each other (maximum 1/3 Byzantine nodes). Meanwhile, the algorithm's nodes have credit rating with scores that will be added or subtracted based on whether the vote is correct or not. The credit rating is used to decide the voting weight of the validators, the addition and removal of new validator, etc.

7.1 Supervision Module

Supervision module provides trading authorization and supervision on chains, which constitutes eID and authorization management service.

● **eID:** eID is a set of system that can executes verification of user's real name identity information and then broadcast the information among alliance parties. The information collected by eID includes user's basic information, financial information and behavioral information. eID is a strong examination of the account holders, which meets the supervision requirements without compromising client's privacy.

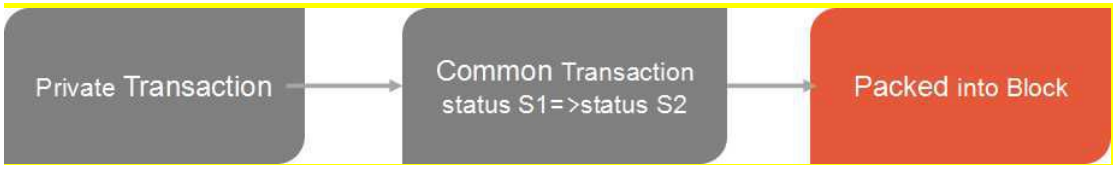
● **Authorization Management:** Authorization management provides authorization and auditing for nodes and transactions. Access management: to provide a complete access management mechanism. According to user's company and title, access management shall give authorization to users by issuing certificate to nodes or authorize encrypted keys. Certificate management: authorize node to join the blockchain network and obtain transaction identity and trading authorization. Certificate management service shall issue three certificates including communication certificate, identity certificate, and the transaction certificate. Communication certificate authorizes node to join blockchain network; identity certificate gives node identity authorization; and only under the transaction authorization can any transaction sent by nodes be executed. Key management:The key management's framework corresponds to the access management structure, different ranks correspond to different levels of key. When user obtains the corresponding certificate, can he apply for the right key in the key management module.

7.2 Privacy Module

Privacy Module provides related services of encryption contracts and various privacy solutions.

● **Encryption Contracts:** Provides encryption contracts solutions for Smart Contracts which have privacy requirements. In encryption contract, messages in smart contract is encrypted, also the

transaction running the contract is encrypted. Private transactions will rely on partial consensus where to implement one private transaction need two steps: the first step is pre-processing, i.e. converting a private transaction to a common transaction [S1=>S2] (S1, S2 are the cipher text status of the smart contract before and after the transaction) , the second step is packaging [S1=>S2] the common transaction into blocks.



Privacy Solutions: Anlink offers various privacy solutions to different user scenario, such as multi-party computation and PGP communication. Through multi-party computation, Anlink can achieve isolated access to private raw data. Through PGP communication solution, Anlink brings fast and secure data sharing service.

7.3 Distributed Ledger

Distributed ledger module contains account service, transaction service, smart contract service and external data service.

- **Account Service:** Account service provides general account service, including address generation and coding, key pair generation and management, signature services, etc.
- **Transaction Service:** Anlink supports three types of transaction: Code deployment transaction, Code calling transaction and Code upgrading transactions. Code deployment is to deploy smart contracts on blockchain, and code call is to execute code on blockchain. What's worth mentioning is that Anlink brings in the concept of code upgrading, i.e. to upgrade the deployed code, in this process, nodes verification must ensure the authenticity and integrity of the execution environment.
- **Smart Contract Service:** Smart Contract service provides smart contract execution providing virtual environment for execution, standardizing contract interpretation logic, and ensuring same execution result for same transactions.
- **External data service:** Traditional blockchain is like an isolated garden in which smart contract could not get external data. To solve this problem, Anlink brings in external data service playing the role of credible data source. Once smart contract has demands for external data, it only need to register in external data service, and external data service shall obtain external data as requested for smart contract.

7.4 Monitor and Analysis

Monitor and analysis module contains three parts: blockchain browser, health monitor and data analysis.

● Blockchain browser: real-time display information of the latest blocks, transactions, contracts and accounts with search function. User can search for related information according to transaction, address, block information, and obtain smart contract illustrations.

● Data analysis: to provide various standardized data inquiry interface and customized service of batch export to meet all kinds of data requirements, such as of auditing, supervision, etc.

● Monitor module: to provide real time monitor on the bottom blockchain's health status, including physical status(CPU temperature, memory, disk), network status(time delay, disconnection), and application status (block generation, transaction verification).

7.5 Storage

Anlink contains two kinds of offchain storage modules. IPFS is used to store large files offchain, while structural storage is used to keep structural records as well ad supporting structural inquiry language.

● **IPFS Module:** To support large file storage, Anlink introduces IPFS technology. Using hash to store files has the advantage of immutability, traceability, anti-leakage and access security, which will guaranty the permanent preservation of user's information, electronic insurance papers, customer information, electronic contracts, property certificates, claims documents, etc., and ensuring data security and user's privacy confidential preservation.

● **Structural storage module:** Structural storage is used to store structural records and to synchronize the records on blockchain.

8 Business Expectations

Blockchain is born with bitcoin, and this is to certify that it is suitable for commercial applications with its inherent attributes. Nowadays, blockchain system can be roughly divided into two categories, one is the digital currency blockchain system represented by bitcoin, and the other is the smart contract digital currency represented by Ethereum. Together with blockchain's immutability, Smart Contract's Turing Complete can execute the contract set in advance as intrigued, and even different people implementing the same smart contract, still they get the same result, thus eliminating differences and creating mutual trust in business. At present, only with separated blockchain systems already make the world feel its overwhelming power. We believe, the Ann-Router System, as an cross chain communication system, will bring much more commercial value to blockchain systems.

Distributed Exchanges

Distributed Exchange is a vital application based on Ann-Router. Centralized Exchanges are

familiar to us, and these Exchanges are already equipped with mature matching system processing high frequency transactions. Trading digital currency on Centralized Exchanges seems reasonable, but in fact, this is a misreading of the blockchain's attributes. As mentioned above, blockchain is prospective on the existing internet architecture, while trading values generated by decentralized network on centralized platform is against the spirit of blockchain.

Of course, restricted by many conditions, Distributed Exchange is still difficult to realize at the moment, but Chain Router at least solved two key issues hindered the development of Distributed Exchange, i.e., transaction speed and cross chain communication. Firstly, Chain Router solved the problem of cross chain communication which builds bridge for cross chain's smart contract coordination. Cross chain communication protocol combined with smart contract guarantee the atomicity of the cross chain transaction, which provides stable communication for every cross chain business. Secondly, AnnCore, which integrates the DS-PBFT consensus algorithm, carries on the block generation by voting with rapid block generation speed in 2-5 seconds per round. Moreover, both Chain Router and Sub-Chain have horizontal scalability, thus the chain network is able to handle cross chain transaction.

It is our belief that the Ann-Router technology is to bring Distributed Exchange into reality and energize digital currency trading with new vitality.

9 Summary

After detailed market research and case studies, we believe blockchain will become a key technology in many industries and further drive innovation, changing the industry infrastructures. Currently, there isn't any complete blockchain architecture that can meet the requirements of high-traffic, regulation, privacy and scalability at the market. Meanwhile, various application cases have different product requirements on the blockchain architecture.

The blockchain routing network is the application of the concept similar to the internet router in information transmission. Ann-Router network can break down the current isolation between different chains, maximally advancing blockchain's potentiality and realizing interconnection, interoperability and mutual trust cross chains.

References:

[1] Economist Staff. "Blockchains: The great chain of being sure about things". The Economist, 18 June 2016.
[2] Morris, David Z. "Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting". Fortune (magazine), 2016-05-23.
[3] Popper, Nathan (2016-05-21). "A Venture Fund With Plenty of Virtual Capital, but No Capitalist". New York Times, 2016-05-23.

[4] Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". https://bitcoin.org/bitcoin.pdf, 2008.
[5] Buterin et al. "A Next-Generation Smart Contract and Decentralized Application Platform". https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper, 2014.
[6] Juan Benet. "IPFS - Content Addressed, Versioned, P2P File System". https://arxiv.org/abs/1407.3561, 2014.
[7] Lamport, Leslie et al. "The Byzantine generals problem". ACM Transactions on Programming Languages and Systems (TOPLAS) 4.3 (1982): 382-401.
[8] Szabo, Nick. "Formalizing and Securing Relationships on Public Networks". First Monday, 6 March 2014.
[9] Goldreich, Oded. "Secure multi-party computation". Manuscript. Preliminary version (1998): 86-97.