Dipper Network: Open Financial Network

Content

Abstract

The birth of Bitcoin has witnessed a whole new era. It deconstructs traditional finance with the idea of point-to-point network and decentralization, and realizes basic functions such as payment, clearing and settlement but this is just the first step in the great vision of blockchain. In today's economic field, lending, money management, insurance and derivative transactions are the most active. However, some shortcoming of traditional financial services, such as,high entry barriers, high intermediate costs, low capital transparency and invasion of information privacy increase financial operation costs and reduce capital utilization efficiency.

Aiming at the problems in current traditional finance, this paper takes Decentralized Finance (DeFi) as the blueprint to solve them. We design a series of basic financial protocols, among which DipBank is an easy-to-use debit and credit application that provides highly liquid and diversified lending services, and it uses a new economic model and open governance model to ease transaction friction and improve capital utilization.

At the same time, the structure, design and performance of the mainstream public chain are uneven, and the assets distributed in the heterogeneous network cannot be interconnected. Based on this, we designed the Dipper Network, a decentralized financial Network, which focuses on building a trans-chain ecological financial center and comprehensively improving the efficiency of asset flow through the design and implementation of sound basic financial agreements. In the future, we believe that blockchains will carry more and more capitals, while the cross-chain Network is a place for transferring and gathering values. Dipper Network aims to create a new financial pattern by rooting in the cross-chain ecology, so that DeFi can bring greater value.

1. Introduction

1.1. Driving factor

Financial systems have existed since the dawn of civilization, and over time they have undergone a great deal of transformations which have changed the forms and principles of

interaction. The financial system evolved from informal savings and loan groups to forms such as cooperatives, mutual insurance and cooperative banks, which through growing, merging and acquisitions later became the well-known commercial and retail banks today. The current financial system is non-transparent, inefficient [1] and is large-scaled. Once risks occur, the society will suffer great influence [2].

The Fintech revolution of recent years aims to reduce this impact by reforming financial markets and creating new community-centred models. Fintech builds highly specialized software where software application and software execution need to be based on trust and subject to restrictions and censorship. Then， the final layer of clearing is a system, not a code. Besides， it does not use encryption to ensure the invariability of the transaction, thus the whole system has a high institutional risk.

Blockchain allows everyone to process and transfer assets over an open network without a trusted third party, unlike to the Fintech architectures available, where blockchain is free and equally available on a global scale, leading to a large and rapidly growing number of digital assets. However, these blockchain assets are faced with mispricing due to limited lending mechanisms and negative yields due to storage costs and risks.

DeFi is built with open source software, and the key logic is run on the trusted encryption network. The builder will not be limited by the financial framework or technology, and in particular, the shortcomings of traditional lending services are optimized. These software all have client-side interfaces that are easier to understand and manipulate and have real-time accessible variable rates, allowing users to interact with the blockchain and thus bringing greater transparency to the transaction process.

Nevertheless, DeFi also faces some obvious problems: first, ecologically, it has low capital utilization and lacks insurance mechanism; Secondly, it is mainly built in Ethereum network, which has led to problems such as network congestion, high transaction costs and uncertainties caused by fragmentation. Finally, each blockchain has its own system so they cannot be interconnected safely and cannot form islands of value, thus making it difficult to form a complete valuable internet.

1.2. Previous work

We will introduce the latest development of blockchain technology and the development of DeFi in recent years.

To begin with, limited by the performance of public chain, there is a lot of work in the field of public chain expansion in recent years, which can be divided into expansion of up-chain Layer 1 and of downchain Layer 2. The earliest Layer 1 scheme is the bitcoin isolation verification (SegWit[11]). Recently, Eether Workshop is preparing to implement Sharding in Casper (Sharding[12]). It is difficult to promote Layer1 in well-known projects, because it involves security issues and multi-party interests. Therefore, Layer 2 scheme has attracted much attention, mainly including State Channel and Side Chain. Typical state channels include the Lightning Network on Bitcoin and the Raiden Network on Ethereum [13]. In the side chain scheme, Polkadot[14] provides a cross-chain scheme of high security, including parallel chain and relay chain, and designs game mechanisms such as dynamic verifier and bounty hunter. Cosmos[15] does substantial work on multi-party cross-chain asset transfer. Each Hub Blockchain serves as the hub of each Zone blockchain communication. It is based on the high-performance Tendermint consensus algorithm. Plasma[16] is proposed by Vitalik Buterin et al which is a side chain with an asset security withdrawal mechanism and meets the requirements of high performance and low security applications whose main chain is responsible for security and state verification.

Second, DeFi is built on the blockchain to provide a financial services system that is accessible to everyone, without barriers or centers. It is Essentially platform-independent, the DeFi applications are developed and used almost entirely on Ethereum in terms of number of applications, volume of transactions, and locked value, with accumulated lock-up assets of over $500 million. Lightning Network[3] is the DeFi application running on the Bitcoin Network. As of July 5 of 2019, the lock-up assets of the flash Network is worth about $8 million. One month after release, EOSrex[4] locked 90 million EOS and enabled users to borrow EOSIO resources such as CPU, memory, and bandwidth. EOS also includes a money market Protocol that does not require license—BUCK Protocol[5]. The first DeFi application on Ethereum is Maker[6], the central bank on the blockchain, where anyone could borrow Dai which is tied to dollar by deposing ETH in their mortgage bond (CDP), with a target value of $1 per token. Compound[7] is a lending agreement known as an automated ethereum firm, in which each money market is linked to an

intermediary cToken (such as a cBAT) that acts as an asset lent out over time. Through cToken, lenders receive interest that accumulates over time. Dharma [7] offer fixed interest rate loans with fixed term. Interest is needed only when the borrower uses the assets. Besides,the platform can trade manual processing and matching, without having to point at any time as custodian, the user can request loan assets, then simply wait for match. Suitable assets include ETH, USDC and Dai. BlockFi [8]provides traditional loan product, and users can obtain legal currency by mortgaged cryptocurrency (the ceiling is determined by the amount of the mortgage), for everyday financial transactions, such as repaying mortgages, buying cars and so on. BlockFi can also make a bigger profit from the loans it makes because it has a bigger loan book. Nexo is a more traditional new cryptocurrency which functions almost exactly like a credit card, allowing those holding cryptocurrency to pledge their cryptocurrency assets in exchange for legal tender credit lines (currently support is not limited to 45 legal tender types). Nuo's [10] function and is similar to Maker-it provides a kind of encryption currency loan agreement, the user can mortgage a kind of encryption currency to borrow another. Unlike Maker, Nuo is not particularly focused on stability or reducing the impact of market volatility.

2. Dipper Network

Open financial system requires an efficient and secure blockchain as a cornerstone. In order to improve handling capacity, Ethereum introduced a shard-chip solution, but Cross slice Trading is complex in design and needs time to be perfected. We therefore proposed and designed the Dipper Network, a high-performance common chain supporting cross-chain technology that would connect to the Cosmos Hub and receive other types of assets from the Cosmos ecosystem. In the future, Dipper Network will connect more blockchains through a variety of cross-chain technologies, including Polkadot, Ethereum, Cardano, etc. Under the premise of security, all kinds of blockchain assets will be received and processed to truly realize the seamless flow of value. In order to further support high-performance applications and improve Network security, we adopted Layer2 scheme in layered design to enable Dipper Network to carry more high frequency calculation and complex computing.

2.1. System architecture

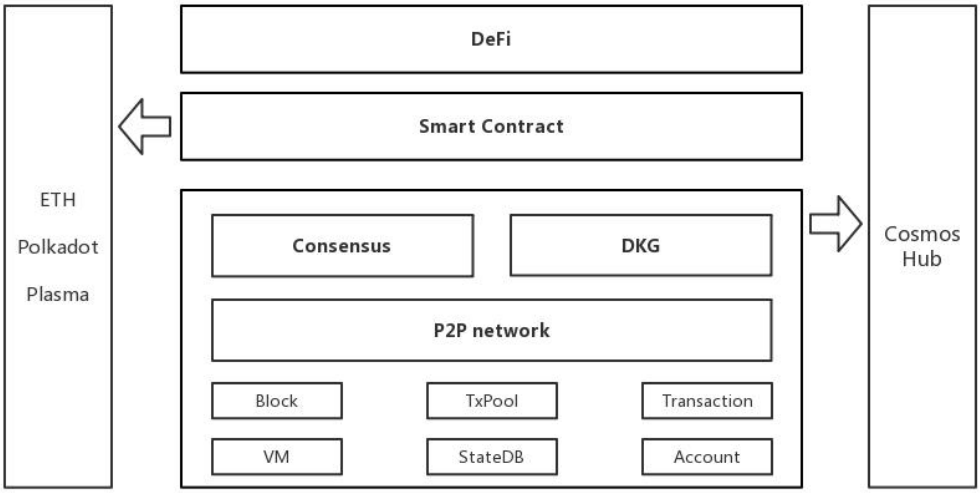

Figure 1:overall system architecture

2.2. Key design

2.2.1. State model

In current blockchain protocols, each node is required to process all transactions and store all states (balances, contract codes, storage, and so on). This approach guarantees network security, but also greatly limits the scalability of blockchain,which means a blockchain network cannot handle transactions that is more than a single node, which leads to degraded performance of blockchain.

After studying the layered network model [19,20,21], we propose a new state model: each transaction contains an event, a state and a proof. By separating calculation and state, state generation is completed off the chain and state verification is carried out on the chain. By using zero-knowledge proof (such as Zk-Stark [17]), general verifiable calculation is realized in the state model, thus reducing the calculation amount of verification on the chain and greatly improving the transaction processing power of the network. The state model of Dipper Network is shown as follows:

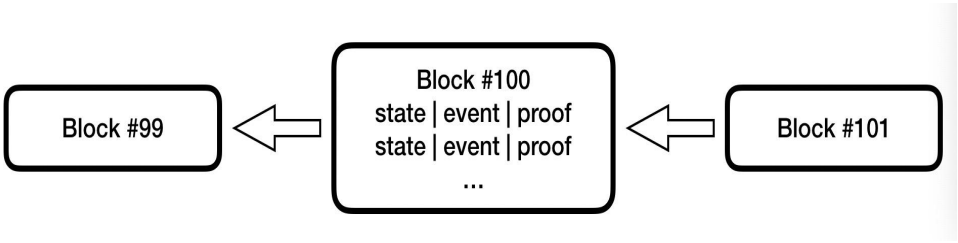

Figure 2:state model

2.2.2. Random number

In order to realize the randomness of bookkeeping and improve the fairness of node bookkeeping and network security, random number is introduced into the consensus algorithm, so a completely fair random number scheme is generated. The block proposer in the consensus process is determined by the random number jointly generated by the consensus nodes. Each round will generate the final signature of the block through the threshold signature algorithm based on BLS, which will be taken as random number and module. The obtained value will be mapped into the sequence based on node equity and accounting efficiency, then the completely random block proposer of the next round will be obtained.

The random number generation scheme uses Distributed Key Generation (DKG), which allows a group of multi-party members to jointly generate polynomials, and each party gets the random key without deviation. The result of the DKG protocol is that each party gets a key pair and shares a public key.

2.2.3. Consensus algorithm

Dipper Network is based on the combination of Tendermint[18] consensus algorithm and DKG then it introduces random number, and has following characteristics:

1) Realize fast transactional confirmation

2) Solve the issues of bifurcation and trade rollback in block chain

3) Achieve higher network throughput

4) Generate fair random Numbers

5) Realize the fairness of bookkeeping

Working as an optimized PBFT algorithm， Tendermint only needs two rounds of voting to reach a consensus. It can also withstand double attacks and tolerate up to a set of the Byzantine

nodes top to one third in a network. The bifurcation accountability system of the Tendermint consensus algorithm can avoid the non-interest problems of the traditional POS algorithm and reduces the risk of malicious bifurcation of nodes. For maximum security and Byzantine fault tolerance, Dipper Network can share the same set of validators with Cosmos Hub.

In the Tendermint consensus algorithm, there are basically two kinds of participants in the network:

1) The verifier, who votes in the consensus process, has different bookkeeping weights;

2) proposal, chosen from fair use random algorithm among the verifier collection. The greater the bookkeeping weight of the verifier, the higher the probability of being selected as a proposal.

2.2.4. Consensus process

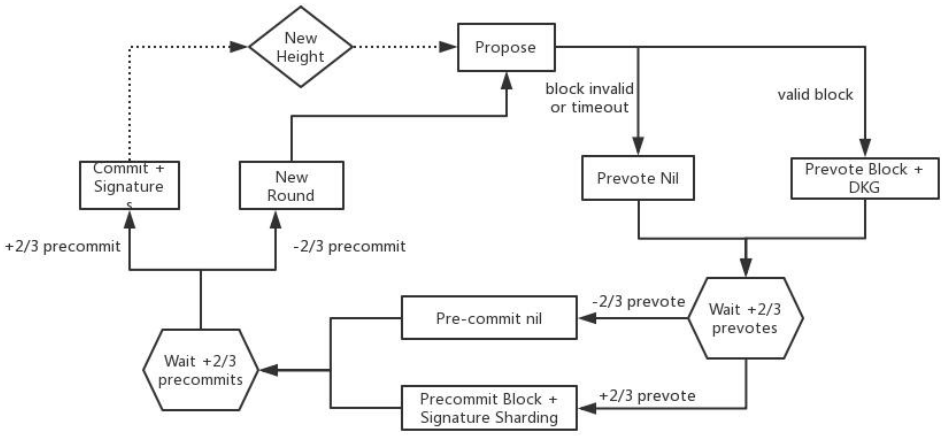

Figure 3:Consensus process

At the beginning of each round, the verifier proposes one new round of blocks. The legitimate proposed block goes through one round of Prevote. After the proposed block gets more than two thirds of the Prevote, it goes to next round: Precommit. The proposed block will be finally confirmed after the pre-submission of more than two thirds of the verifiers.

DKG is introduced during initialization to generate keys shared by all parties. In pre-commit

phase, we use the shared key above to generate Signature Sharding based on the BLS threshold signature algorithm, and merge it into a final Signature in the final submitted block. Only when random Numbers are generated through multi-party co-worked signature with characteristics as uniformity, mutual independence and unpredictability can serve as fair random Numbers in the chain.

2.3. Cross-chain solutions

Dipper Network will realize asset cross-chain only through the block chain protocol itself, without the involvement of a third party (such as centralized exchange). Currently, Cosmos and Polkadot are the most promising blockchain cross-chain projects, which have been deeply engaged in cross-chain fields for many years and have a good reputation in decentralized communities. Dipper Network will connect with Cosmos, Polkadot and more block chains, so that all kinds of encryption assets can flow in, giving full play to their financial values.

2.3.1. Cosmos cross chain

Dipper Network supports cross-chain asset within Cosmos ecosystem, connecting Cosmos Hub through IBC, and thus achieving communication with Zone blockchain which is connected to Cosmos Hub in the form of Zoning. Dipper Network will also implement Peg Zone to allow real-time blockchain (such as Ethereum) to connect to the Dipper ecology.

Taking the cross-chain transformation of Dipper Network and Ethereum as an example, it can be divided into two processes: cross-chain between PegZone and Ethereum, IBC cross-chain in the Cosmos system. Figure 4 describes PegZone and Ethereum cross-chain transfer process. In this case Alice transfers 10 Eth through the Ethereum chain to PegZone block chain, in the exchange of PegZone CEth assets equivalent of 4 Eth to Bob. Bob in PegZone performed redemption transaction and then PegZone chain, Signer, Layer components all validate to Bob's operation, give signature and notice the Ethereum smart contracts. After ethereum Smart contract was verified, signed, and traded, it will release four Eth to Bob.

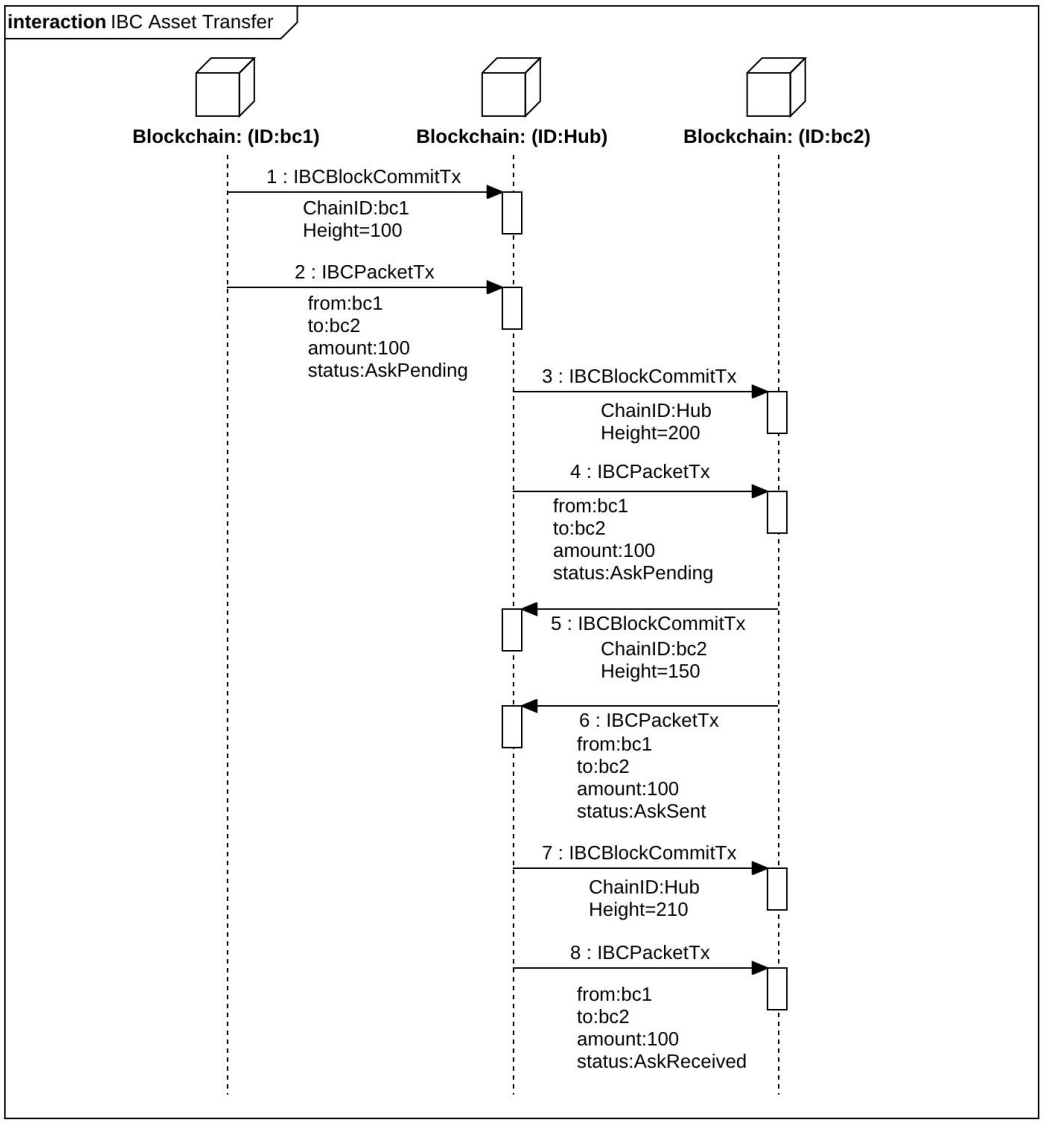

Figure 4:Cross-chain transfer process of PegZone and Ethereum

1) Dipper Network creates smart contracts in Ethereum to record and process the logic and data of Eth transfer across the chain

2) Alice performs cross-chain transfer through ethereum smart contract to transfer 10Eth to its address in the PegZone public chain

3) Pegzon-related Witness components notice this trade and continue to listen until the trade is irreversible in Ethereum Public chain

4) Witness sends ALice's cross-chain transfer request to PegZone

5) After PegZone verification transfer passes, it issues 10 CEth to the address (here refers to

ALice's address in PegZone, which can be any address) in the transaction request to indicate that it has received 10 Eth value assets

6) After Alice is informed that the cross-chain transfer was successful, she transfers 4 CEth to Bob's address through PegZone

7) PegZone verifies the transaction and executes Alice's request

8) After Bob receives the transfer from Alice, he begins to perform the redemption request (representing the redemption of assets from PegZone chain to Ethereum)

9) Signer component listens to Bob's redemption request, signs the transaction and sends its own transaction request to PegZone

10) Layer listens to Signer's trades until 2/3+ votes confirm the trades

11-12) After Layer confirms that the redemption transaction request is irreversible, it starts to execute the forward transaction request to Ethereum smart contract (invoke Ethereum smart contract interface)

13) Smart contract releases 4 Eth to Bob's Ethereum address with logic

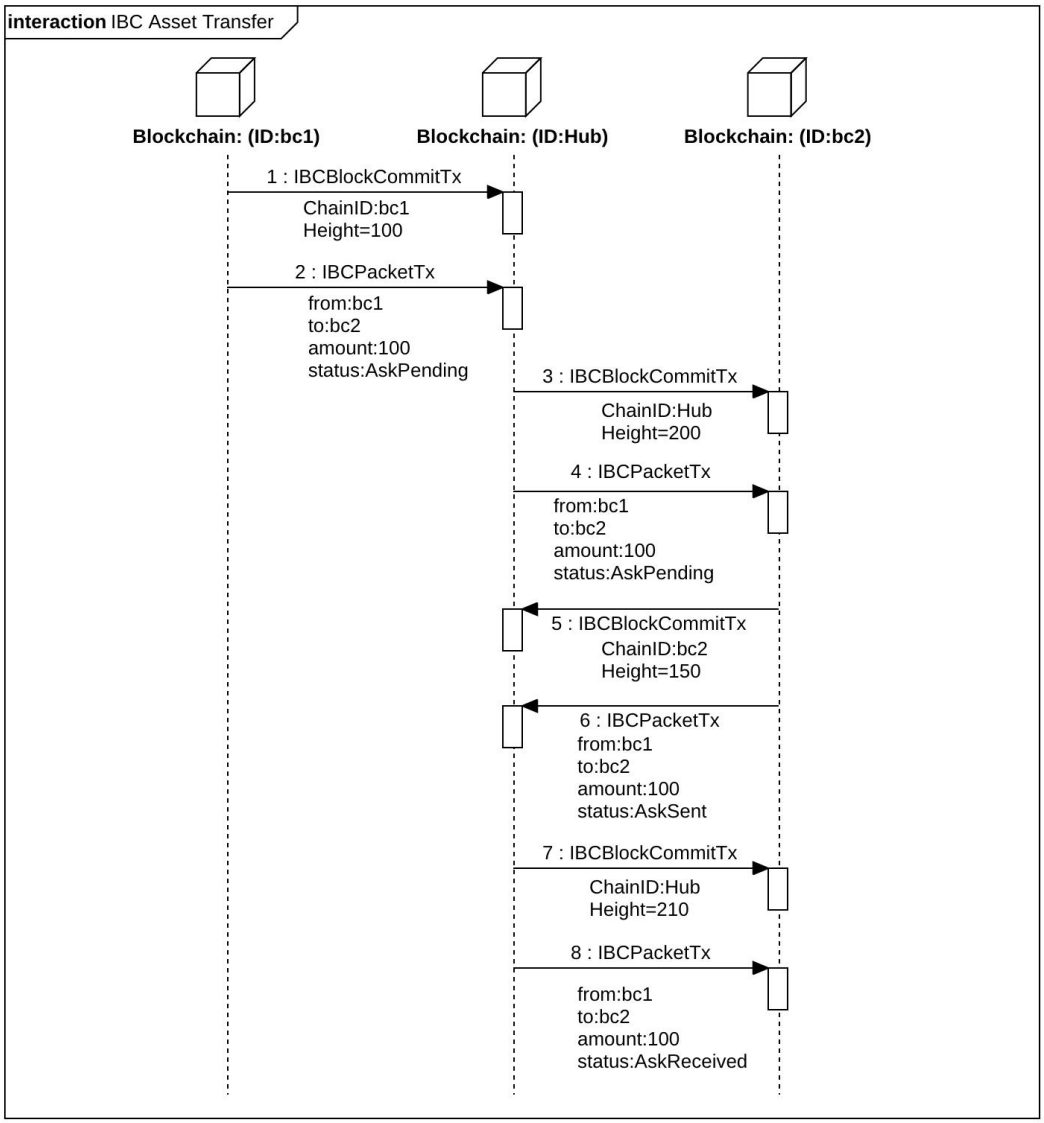

Figure 5:IBC cross - chain transfer process in Cosmos system

1) bc1 chain sends block height information to Hub chain

2) bc1 chain initiates a cross-chain asset transfer transaction. The asset transfer direction is bc1-> bc2, and the number of assets is 100 single bits. The status of the transaction is AskPending. After bc1 verifies the successful transaction, it will put the transaction request into the hub-oriented trading channel.The repeater listens to the trade request of the trade channel to generate Merkle Proof as the IBCPacketTx payload and send it to the Hub

3-4) Hub verifies the IBCPacketTx received in step2, and sends the block height information of the Hub and cross-chain transfer transaction to bc2 through the logical step of step1-> step2

after verification

5-6) After bc2 receives Hub's transaction request, it verifies the transaction. After the successful verification, it synchronizes the block height information and the idea that it can accept the transfer request transaction to the Hub

7-8) Hub sends block height and executes asset transfer transaction to transfer corresponding amount of assets to bc2 to complete cross-chain transfer business.

2.3.2. Polkadot cross chain

As an inter-blockchain protocol, Polkadot allows independent blockchains to seamlessly trade and exchange information in an untrusted manner through a heterogeneous multi-chain architecture. Dipper Network gets through Polkadot Network through the cross-chain mode of transfer Bridge and Relaychain. When Dipper Network node sends information to other block chains, data will be passed to the Relaychain through the Bridge (Bridge). After several routes, Relaychain finally finds the correct Parachain, which will be verified by the Validator, and the information will be calculated and processed.

Each parallel chain has the same complete node responsible for a specific parallel chain, known as collator. These verifiers collect and validate transactions from users, and then transmit the verified transactions to participants in the Relaychain, the Validators, who run the equivalent of light nodes on the Relay chain and are responsible for validating and broadcasting the blocks sent from the verifiers. In order to ensure the verifier to make the right behavior and do not broadcast invalid trading, another kind of participants is introduced, which is referred to as fisherman. They earn bonuses as long as they prove errors of validators

The workflow of a transaction from one parallel chain to another is as follows:

1) The user creates a transaction on parallel chain A to send information to parallel chain B.

2) The transaction is sent to a collator in parallel chain A.

3) The collator ensures that the transaction is valid and includes it in a block.

4) The collator display this block and a proof of state transition to a validator at the parallel chain A.

5) The validator verifies that the block received contains only valid transactions and mortgages their DOT tokens.

6) When there are enough nominees to mortgage their DOT tokens and nominate validators, broadcasting their blocks to the relaychain will be authorized.

7) The transaction was animating and at the same time the data from parallel A was transmitted to parallel B.

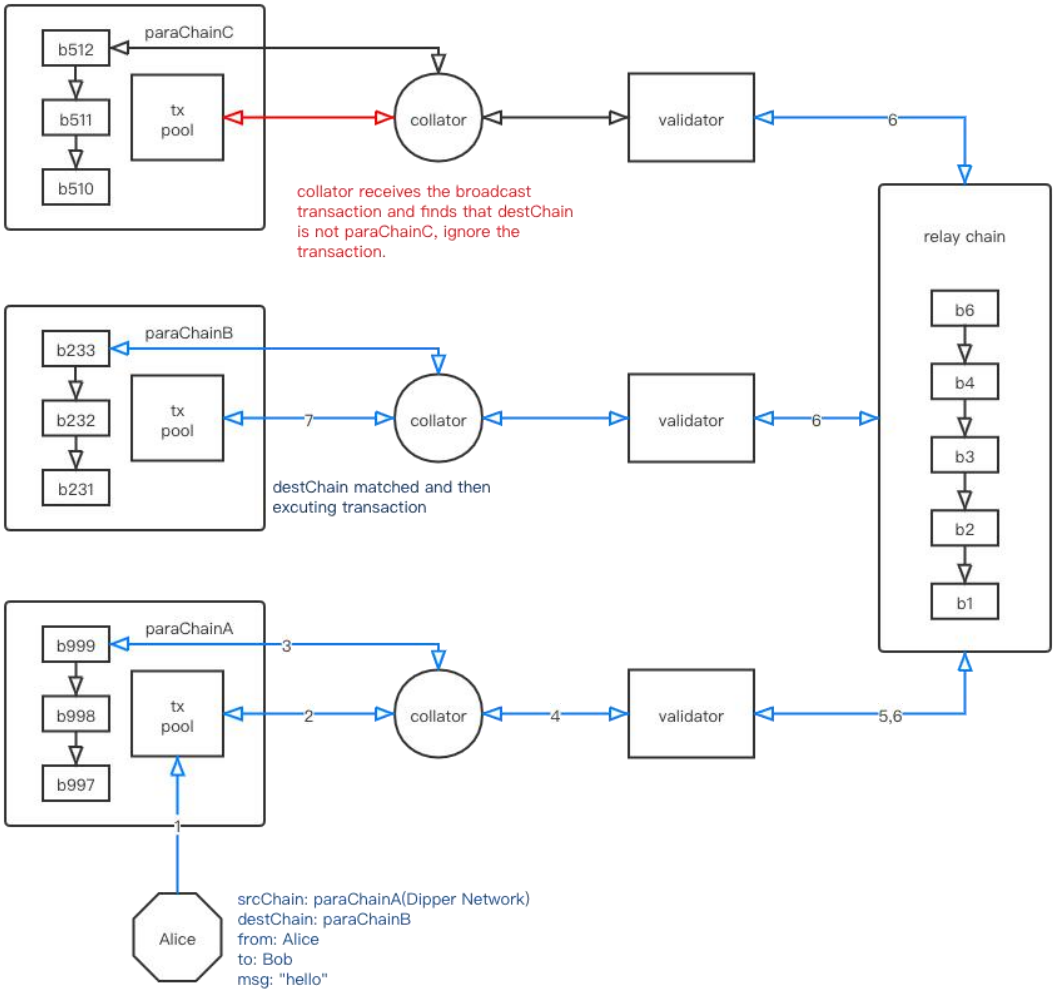

Figure 6:Cross-chain communication process in Polkadot

2.3.3. Layer2

The current public chain hits a significant bottleneck in the transaction processing capacity, and even Cosmos will struggle to meet the needs of growing and diverse commercial applications in the future. Mainstream solutions nowadays include Sharding based on Layer 1 and State Channel or Plasma based on Layer 2. Sharding is complex in design, easy to cause security problems such as network partitioning and has many restrictions on cross-chip trading. Therefore,

we choose Layer 2 to layer the consensus and focus on security and state verification on Layer1. Focusing on performance and state generation on Layer2 fosters greater concurrent business and security.

Dipper Network will implement Layer 2 which is based on Plasma: Plasma contracts will be deployed on the root chain to define rules such as recharge, withdrawal, block proof and fraud proof. When malicious activity is detected on the side chain, the user can invoke Plasma contract to safely retrieve assets on the root chain, and the side chain runner will be penalized. Plasma has also designed a series of economic games , such as withdrawal delays and pledging funds for fraud proof or withdrawals. The overall process is as follows:

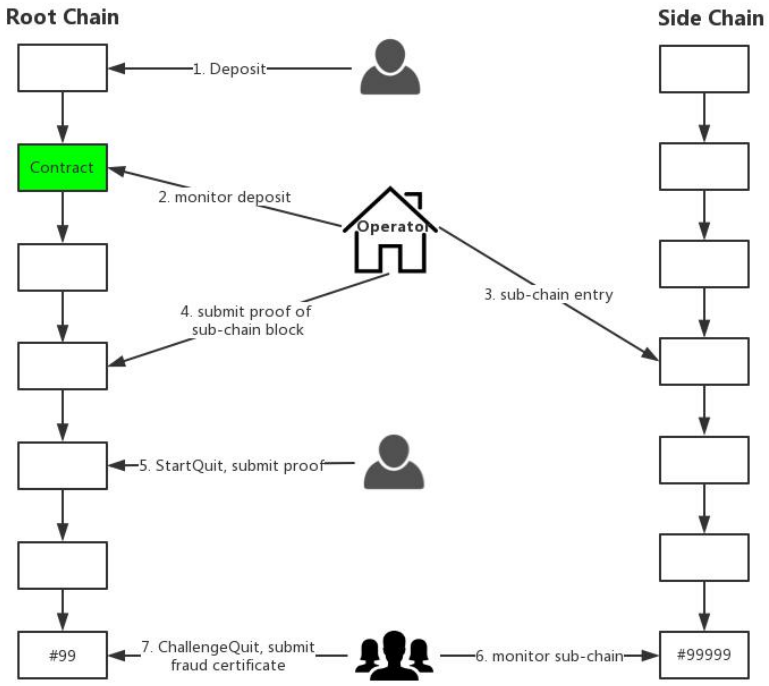

Figure 7:Layer 2 program flowchart in Dipper Network

1) Root chain user invokes Deposit to recharge the Plasma contract, and the asset will be locked in the contract;

2-3) Operator listens to the contract, checks the asset lock proof in the contract, and credits the account for corresponding user on the subchain;

4) Operator regularly submits block certification of the side chain to the Plasma contract.

Any user can submit fraud proof to the Plasma contract. When the contract is verified after the agreed dispute period, block submitted by the operator will be cancelled and he will be punished

5) Users can quit the subchain at any time and invoke StartQuit to perform withdrawal operation and retrieve legitimate assets. There is a dispute period (7 days).

6-7) During the dispute period, other users can invoke ChallengeQuit to challenge. If challenge succeeds, the challenger obtains the quit deposit of the user, and the user fails to quit and the deposit is deducted; if users quit successfully, the Plasma contract sends the legitimate assets to the user that give out quit request.

3. DeFi Dapps

The debit and credit applications in DeFi ecosystem are mainly divided into two mainstream modes: capital pool and P2P mode. Compound is typical in the capital pool model with dynamic interest rate setting and good liquidity, but it has less types of mortgage and accounting standards cannot maintain the first-mover advantage. Dhrama is the most active application of P2P model. It simulates the traditional lending model and provides a variety of 90-day regular lending services. However, the source of currency information, the determination of interest rate, and the development and update of the platform are too centralized. Based on the above considerations, we combined the advantages of the two and designed DipBank: a fully functional and easy-to-use lending application. On the one hand, it has both demand and fixed services, which can maximize the utilization of funds while ensure security. On the other hand, it has a new Token incentive mechanism and promotes the effective balanced distribution of DIP. Detailed design is as follows:

3.1. DipBank

3.1.1. Lending assets

1) In demand products, we have designed a capital pool to provide efficient capital liquidity and there is no need for the borrower and lender to design a loan contract or wait for the loan to mature. Users can invoke the saving tokens to store the assets supported by the system and they become substitute resource and users can invoke the borrowing tokens to borrow assets.

2) users can invoke createFund Tokens to meet the investment needs of fixed interest rates in

term products by setting up cycle, interest rate as well as amount and other information. Other users can invoke supplyFund Tokens to participate in term financial products.

In the system, dToken is used to replace the user's assets. In demand products, the amount of dToken will increase correspondingly as interest is generated in the money market.

3.1.2. Borrowing assets

Using dTokens as mortgage, users can transfer borrowing assets from DipBank to anywhere on the Dipper network. Similar to providing assets, each money market has a floating rate set by market forces, which determines the cost of borrowing for each asset. There are two types of borrowing assets:

1) In a demand product, marketBorrow can be invoked on a MoneyBank contract by the user who wants to borrow and has an adequate balance stored in DipBank. This function invoke will check the user's account value, give enough mortgage, update the user's borrowing balance, and transfer token to user's Dipper address, and at the same time update the floating rate of interest in the currency market. The way that the borrowing assets' generate interest will be the same as the one calculated in 3-3

The borrower can invoke RepayMoney at any time to repay the principal and accrued interest on the outstanding loan.

The assets held by the agreement (represented by the ownership of dToken) are used as mortgage to borrow from the agreement. Each market has a mortgage factor X, ranging from 0 to 1, representing the value of the underlying asset that can be borrowed in. According to the liquidity of funds, we set the mortgage factor X of different assets, and the subsequent parameter will be set by the management committee. The user's ability to borrow is equal to the sum of the balance values times the mortgage factor.

2) In term wealth management products, the borrower calls marketFund (asset address, amount of money, interest rate and term) on the MoneyMarket contract. This function is invoked to check the user's account balance and give enough mortgage to set the user's borrowing amount. The interest rate on the loan is freely specified by the user, and the borrower will automatically repay the outstanding loan at the end of a given period. If the borrower pays for the loan in advance, interest for a given period will be charged.

If the value of the user's overall account is lower than the liquidation rate due to changes in the value of their mortgage (for example, the user holds DIP as mortgage to borrow ethereal and the DIP significantly reduces its value) then we have a public function liquidateBankBorrow to exchange the borrower's assets for the borrower's mortgage at a rate 5-10% below the market price.

3.1.3. Books and interest rate models

DipBank's current product imitates Compound which takes international industry-leading accounting standards and has a complete and audited balance sheet and account ledger for each money market:

$$Supply + Equity = Cash + Borrows \quad (3\text{-}1)$$

In periodic product mode, it is customed by borrower. In the demand product model, dynamic interest rates are used. According to economic theory, interest rates should rise when demand is high and fall when demand is low, and capital utilization should be used to measure the strength of demand.

$$userRatio = borrowingBalance / (borrowingBalance + cash) \quad (3\text{-}2)$$

$$borrowInterest = P1 + userRatio*P2 \quad (3\text{-}3)$$

$$lendInterest = borrowInterest*userRatio*P3 \quad (3\text{-}4)$$

P1, P2, P3 will be decided by Governance Committee. Each time a transaction occurs, the interest rate on the asset will be updated to compound the interest since the previous index. The period interest calculated at r * t per block will be computed:

$$Indexn = Index(n-1)*(1 + r*t) \quad (3\text{-}5)$$

The total outstanding borrowings of the market are updated and the accumulated interest since the last index is included.

$$totalBorrowBalancen = totalBorrowBalance(n-1)*(1 + r*t) \quad (3\text{-}6)$$

3.1.4. State of market

Each market (defined by assets) contains three states: prepared, operating, or suspended. If, for any reason, the state of the market must be changed, the corresponding proposal will be discussed and decided by the governance committee. Besides time for users to prepare should be

provided prior to that. Suspended markets do not allow users to continue to supply or borrow assets (although users can still withdraw or close borrowed positions).

1) Prepared: Each market will begin with preparation and possibly transit to a support state. Once the market is in support state, any user can supply or borrow from the market as described above.

2) Operating: The market operates normally in this state, supporting for the supply and borrowing of assets. Operating status would be up to the governance committe to decide whether to switch to a suspended state in the event of a predictable risk to prices from lending.

3) Suspended: Once the market is suspended, all borrowings on the asset can be liquidated at a standard discount, regardless of the borrower's mortgage condition.

3.1.5. Governance

From the initial stage, DipBank was controlled by the DAO elected by Dipper Network. DAO will take the form of smart contract and invoke following functions through proposals and votes. The following rights in this agreement are controlled by the Administrator or the Governance committee:

1) Select new committee members

2) Set the interest rate model of market

3) Prepare, suspend or cancel the market

4) Select Oracle price source

5) Activate the overall market clearing

6) Accept the contract or not

3.1.6. Risk and liquidation

If we set the mortgage rate as 150%, and the DIP holders can vote on the mortgage rate for each type of asset. When borrowing occurs, the following three situations occur:

1) When the mortgage rate is higher than 150%, the system will operate normally;

2) When the mortgage rate is lower than 150%, the liquidation mechanism will be triggered, and the mortgaging asset-dToken will liquidate the current market price minus the liquidation discount. The incentive is for arbitrageurs' rapid ecosystem intervention to reduce the borrower's

risk and eliminate the risk of protocol. The percentage eligible for closure is closely related to the percentage of borrowed assets that have been repaid on a scale of 0 to 1, 25% for instance. You can continue to invoke the liquidation process until the user borrows less than he can borrow. Any address that owns the borrowed assets can call the clearing function to swap their assets for dToken mortgage from the borrower. As users, assets and prices are included in the Bank agreement, and the liquidation is not dependent on any external system or order book.

3) When an extreme event happens and the mortgage rate falls below 100% at a sudden, the system will suspend the market and activate the preset risk reserve to subsidize users.

3.1.7. Token motivation and distribution mechanism

We designed the lending incentive algorithm, which means that lender and borrower will not only obtain or pay the interest, and the DIP will be given as the incentive, and it will be subsidized to both lenders and borrowers according to the interest rate. Token incentive to promote lending is conducive to promoting the positive cycle of Dipper network, so it helps improving the utilization rate and security of the network, and thus forming a stable economic closed loop.

3.2. Basic financial agreement

We will further build a complete basic financial agreement on Dipper Netowrk:, including stablecoin (DipUSD), de-centered exchange that offers liquidity(DipDex), important derivatives market (DipDER), synthetic asset(DipSYN), perfect asset insurance service(DipINS), oracle machine that provides reliable external information(DipORC), etc.

4. Economic model

Economic models are the soul of the public blockchain. By introducing economic incentives, Bitcoin solved the consensus problems of the open network for the first time. Each blockchain network is an autonomous community bound together by economic incentives. An excellent economic incentive system should guide blockchain participants to contribute to this autonomous community, maximize the utility of blockchain, and motivate users, developers and node operators to jointly contribute to the formation and preservation of consensus.

Dipper Network supports both smart contract and multi-token model. Token will be stored in all blocks and can be moved from one to another through the Dipper Network. In the initial stage, there are two types of tokens that can support Dipper network. They are Staking Token and Fee Token.

4.1. Staking token

Staking token uses a collateral mechanism similar to Cosmos network [15], Dipper Network has its own special local token for collateral, which is named "DIP". DIP can be used in a variety of situations, such as:

1) The DIP token can be integrated into the consensus engine validators in Dipper Network through validator and Client system.

2) The DIP token can participate in the governance of Dipper Network;

The security of Dipper Network is closely related to the number of tokens collateralled in Consensus Nodes. More collateral tokens by consensus nodes means higher evil cost of the nodes and the whole system will be more safe. The DIP also represents the storage resources on the Dipper Network. If there is more DIP, there would be more state space so as to effectively deal with the state explosion problem, which is conducive to the long-term operation of the system and effective acquisition of the value on the chain.

4.2. Fee token

Network fee tokens are used to prevent spam and pay the validator when maintaining the ledger. Dipper Network aims to support all tokens on the white list recognized by the Cosmos network, such as Photon token and IRIS token.

An important reason why it is difficult for mainstream users to use blockchain is that transaction fees must be paid in native currency, which requires users to find a way to obtain the native currency first before using the service, which raises the threshold of use. On the other hand, users have been accustomed to free basic services and charging for value-added services. Charging for every service is not in line with users' habits. We plan to adopt the feature of Cosmos to support various white-listing fee tokens that provide better experience for network users. In Cosmos, each validator has a configuration file that defines their individual weight for the value of

each fee token.

The portion of the commission fee will be determined by a vote and a majority of income will be earned by outbound nodes. The rest will be used to develop, research, and operate Dipper network to ensure the normal development of the network.

5. Development plan

The development plan for Dipper Network consists of the following stages.

In the first stage, Dipper Network testnet will be launched.

In the second stage, the official web will be launched.

In the third stage, DipBank and DipDEX will be launched.

In the fourth stage, the IBC protocol and heterogeneous network cross-chain scheme will be customized.

In the fifth stage, a complete DeFi infrastructure will be implemented.

In the sixth stage, a comprehensive and inclusive financial network service will be launched.

Conclusion

We believe that because of the trend of expansion in blockchians to support the commercial-grade applications, any public chain would not be effective in loading all value thus there is a own unique business hub formed by some head public chains. And cross-chain will be as a core, connecting all kinds of public chains, converging value to produce scale effect. So we will build Dipper Network into cross-chain ecology, focus on financial applications and redefine the decentralized financial to benefit everyone from financial.

We create a functioning money market for cryptoassets through DipBank, where interest rates are determined by the supply and demand of capital. When demand for borrowed assets increases or the supply decreases, interest rates will rise, encouraging additional liquidity and then users can offer tokens to the money market to earn interest without trusting intermediaries, and users also can borrow (use, sell, or re-lend) tokens in the agreement. We also design an innovative Token distribution mechanism to subsidize users and build a network economic ecology, so as to

avoid cold startup. At the same time, we design a completely centralized mechanism to enable Token holders to deeply participate in governance.

In the future we will work on following aspects. First, we will delve into cross-chain mechanism and integrate advantages of various cross-chain schemes to improve safety. Secondly, complete basic financial facilities will be constructed and standard interfaces should be designed to enable efficient combination of various types of applications. Thirdly, Zkp will be studied deeply to realize the universal verifiable computation. Fourth, we will enhance scalability and optimize Layer2 solutions; Fifth, We will try to support privacy transaction, such as mimblewimble protocol; Sixth, we will optimize encryption economy to better anchor the assets on the chain and the underlying public chain.

Core member

Huang Zhiyong	CEO	Former chief researcher of GXChain, Former engineer of China Mobile Research Institute in Hangzhou, serial entrepreneur
Luo Tianjia	CTO	High street fashion technology director, former outstanding engineer of Huawei, serial entrepreneur
Zhu Liting	Conselor	Former chief architect of Gong Xin Bao, Graphene community developer, technical consultant in global graphene blockchain application center
Yang Chao	Operator	Well-known currency circle KOL, former senior operational manager of NetEase
Hou Jinwei	Business	Well-known community operational promoter, serial entrepreneur

Acknowledgement

Dipper's design has gone through many iterations and evolution, and it is based on the work of Dipper Labs developers. We would like to thank all of you for your contributions during this

process. We also appreciate developers in the Ethereum community, Cosmos community,as well as the Polkadot community for your dedicated work.

Let us work together to create a better future!

Reference

[1] TresuaryDirect. The data on total public debt outstanding 1993-2019.

[2] The coming pension crisis. Citi GPS: Global Perspectives & Solutions, 2016

[3] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable offff-chain instant payments. Tech. rep. Technical Report (draft). https://lightning.network, 2015.

[4]https://eosrex.io/

[5]https://medium.com/@dmitry.yunodo/buck-protocol-is-live-fef2cf5765d7 ↩

[6]Maker Team. The Dai Stablecoin System (2017). https://makerdao.com/whitep aper/DaiDec17WP.pdf

[7]https://www.dharma.io/

[8]https://blockfifi.com/

[9]https://nexo.io/assets/downloads/Nexo-Whitepaper.pdf?n=2

[10]https://www.nuo.network/

[11] Eric Lombrozo, Johnson Lau, Pieter Wuille. Segregated Witness (Consensus Layer). https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki. 2015.

[12] Sharding FAQ. https://github.com/ethereum/wiki/wiki/ShardingFAQ, 2016.

[13] “Micro-raiden: A payment channel framework for fast and free offff-chain erc20 token transfers.” [Online]. Available: https://raiden.network/micro.html

[14]Gavin Wood. POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK. https://github.com/w3f/polkadot-white-paper/raw/master/ PolkaDotPaper.pdf, Nov 2016.

[15] Jae Kwon jae, Ethan Buchman. Cosmos: A Network of Distributed Ledgers. https://cosmos.network/cosmos-whitepaper.pdf, 2016.

[16] Poon J, Buterin V. Plasma: scalable autonomous smart contracts. See https://

plasma.io/plasma.pdf. 2017.

[17] Eli Ben-Sasson, Iddo Ben-Tov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. https://eprint.iacr.org/2018/046.pdf, 2018.

[18]J. Kwon. TenderMint: Consensus without Mining, August 2014.

[19] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Jonathan Kat z and Hovav Shacham, editors, CRYPTO 2017, Part I, volume 10401 of LNCS, pages 357–388. Springer, Heidelberg, August 2017.

[20] Will Martino. Kadena: The first scalable, high performance private blockchain, http://kadena.io/docs/kadenaconsensuswhitepaper-aug2016.pdf, 2016.

[21] Jan xie. Nervos CKB: A Common Knowledge Base for Crypto-Economy.

Legal statement

Dipper Network Tokens is only a medium of exchange for specific groups or participants. It is not a prospectus or offer document of any kind. Nor is it intended to constitute a unit of securities offer in any form or in a business trust. Nor is it a unit in a collective investment plan or any other form of investment or any form of investment offer in any jurisdiction. No regulatory administration has censored or approved any of the information set out in this white paper.This white paper has not been registered in any regulatory authority in any jurisdiction. Accessing and/or accepting any information in possession of this white paper or part thereof, you meet the following criteria by default:

A) You are not a citizen or resident of the People's Republic of China (in terms of tax or other), or reside in the People's Republic of China;

B) You are not a citizen, resident (tax or otherwise) or green card holder of the United States of America, or resident in the United States of America;

C) You are not in a jurisdiction, whose laws, regulations or rules announce that the sale of token in any form or manner is prohibited, restricted or unauthorized, in whole or in part;

D) You agree to meet the conditions and constraints described above.

Risk warning

This information does not represent investment advice, or permission to sell, or guidance to attract any purchase.

Term list

DeFi	An ecosystem of applications built on permission-free blockchains, point -to-point protocols, as well as decentralized networks, which aims to facilitate lending and other financial transactions.
Plasma	A scheme that aims to realize the expansion of blockchains. It can realize automatically persistent state on the chain by creating economic incentives, without the state transition management by contract creator.
DKG	Distributed Key Generation; Distributed key generation algorithm is for generating shared keys in nodes of distributed systems.
BLS	A short signature algorithm; the main idea is to place messages to a point on an elliptic curve and verify the signature without revealing the private key by using the exchange property of bilinear mapping function. BLS algorithm has rich applications in signature merge, multi-signature as well as m/N multi-signature.
MPSS	Mobile Proactive Secret Share; a mobile active key sharing algorithm which is used to dynamically update and transfer keys between different node groups.
VRF	Verifiable Random Function; it is put forward by Micali, Robin and Vadhan and it is a pseudo-random function, which provides open and verifiable proof of its output.
VC	Verifiable Computation; this can effectively verify whether the resulting data is calculated in accordance with the original data and specific logic.
Zkp	Zero-knowledge Proof; the certifier assures the verifier that a fact is correct and does not reveal any other information(Zero knowledge)