

# Biconch Chain: A New Distributed Web Protocol Based on an Innovative Proof of Reputation (PoR) Consensus Algorithm and Eco System

Authors: Caesar Chad\*, Neo Liu\*, Leon Lau\*, Joseph Sadove\*

July 24, 2018

## Abstract

BITCONCH chain proposed an innovative POR (Proof Of Reputation) reputation consensus algorithm, which solved the pain point that the blockchain is difficult to maintain both high throughput and decentralization. Based on social graphs, BITCONCH Chain mathematically models social, time, and contribution activities to build a decentralized reputation system. Each user has the opportunity to establish a high reputation value. The higher the user's reputation, the lower the transaction cost (or even free). The more opportunities that are selected as trust nodes to participate in the consensus, the greater the benefits. High-reputation users are defined as “mutual trust nodes”, and small micro-transactions will start “payment channels” for high-speed offline transactions.

The reputation system and system incentive system will effectively promote the continued enthusiasm of business developers and ordinary users, and contribute to the construction of the business ecosystem. Business developers with traffic are more likely to get high reputation values, and the chances of being elected to a trusted full node are higher. Ordinary users can increase reputation by actively engaging in social interactions

---

\* Bitconch Blockchain Technology Ltd, [info@bitconch.io](mailto:info@bitconch.io)

and actively using business applications in the ecosystem, increasing the chances of being selected as trusted light nodes.

The Bitconch chain uses a DAG directed acyclic graph data structure to maintain the system's positive scalability. Support smartphone light node client to resist the decentralization of the system and maintain dispersion. Zero-knowledge verification, latticed data storage, quantum-level encryption algorithms, and improved BVM virtual machines make Bitconch chain more reliable and provide a friendly DApp and sidechain development environment to meet certain applications. Technical requirements for large file storage, low transaction costs, user information protection, sidechain and smart contract iterations, and bug fixes.

BITCONCH chain is a decentralized distributed network with no block and no chain, which solves two difficulties in the application of blockchain: scalability and decentralization. Bitconch chain, which can be applied to the commercial application needs of users above 10 million, is the most feasible blockchain ecosystem for high-frequency small micro-transactions and social applications.

## **1. Background**

The birth of Bitcoin has made blockchain technology leap from pure theoretical research to the world's focal point of innovation and technology. The blockchain is believed to be a technology which will dramatically change the world. The success of Ethereum, which proposes smart contracts for developers to develop an application on the blockchain. However, due to the limitations of many technical bottlenecks, the current blockchain is still far from large-scale commercial adoption, since commercial applications may need to address the following technical bottlenecks:

- Scalability
- Decentralization
- File Storage
- Low Transaction Cost and Effective Incentives

- Upgradable Smart Contract
- Privacy Protect
- System Securities
- Usability

## **2. The Challenge Of Blockchain In Real World Applications**

### **2.1 High Concurrency, High Throughput And Scalability**

The core of business competition is traffic competition. A successful business project usually has more than 10 million registered users and more than one million active users. The scalability problem of the blockchain, that is, how to increase the speed of transactions and the throughput of transactions, which is the focal point of current researches. Multiple applications (DApps) in the ecosystem may generate high concurrent requests, and system throughput should be at least tens of thousands of transactions per second, which could reach the level of Visa/MasterCard.

### **2.2 Business Reputation And User Privacy**

Blockchain technology was hailed for its anonymity. By hiding the identity of the users, Blockchain can protect the user's privacy. However, in real business applications, pure anonymity may bring problems such as fraud, breach of contract, and difficulty in defending rights. When a user chooses a service provider, they have the right to know whether the service provider is honest and trustworthy.

### **2.3 Incentive Mechanism And Transaction Costs**

The business application scenario is mainly for high-frequency small and micro-transactions of small and medium-sized users, so transaction costs will become an important consideration. The transaction cost of Bitcoin has exceeded \$1/transaction, and the transaction cost of Ethereum is 0.01~0.02ETH/transaction, which is about 5~10 USD/transaction. Excessive transaction costs are clearly unable to meet the

commercial needs of high-frequency micro-transactions.

Consumers may wish to use the resources on blockchain platform, for free or at low price, but there is a clear conundrum, for a decentralized system, there is no central authority to maintain the system, so an effective incentive mechanism, which keeps the peers participating in the activities that keep the system as a whole working instead of just doing what benefits an individual, is essential to the system. The peers need enough incentives to pay for operating costs (including equipment and utility fees) and maintain a constant enthusiasm for participation to maintain the decentralized system decentralization. How to effectively balance the contradiction between the two is the key to building a sustainable underlying system.

## **2.4 Security And Decentralization**

In order to ensure transaction security, each client needs to download and back up the transaction data of the whole network, which is called "Full Node". However, running a full node in most cases is extremely expensive and slow, and most users in commercial applications are dealing with small and micro transactions, and have no ability and demand to purchase large computers and bear the corresponding operating costs. Therefore, small and medium-sized users are effectively blocked from participating in system computing process (consensus process etc.) and cannot obtain system rewards, thus forming a monopoly of computing power for a small number of rich users.

## **2.5 Upgradable Smart Contract**

Applications developed on the blockchain need to have a reasonable mechanism to support software upgrades when iterating over functions. All software is likely to be affected by bugs. When a Side Chain or DApp encounters a bug, it needs to be able to fix the errors from the bug.

## **2.6 Limitation On Storage**

The development of many commercial applications often involves large file storage and transmission. For example, applications such as media, social software, e-commerce

platforms, live video, games, etc. require large file storage functions. The classic blockchain does not support the storage of large files, and cannot meet the demands of real-world applications.

### **3. Proof Of Reputation Consensus Algorithm**

The POR reputation consensus algorithm is a new algorithm proposed by BITCONCH based on social graphs. Using a distributed decentralized reputation quantification system built on the blockchain, POR can show the contribution of each peer to the whole network, including growth, security, and stability. By introducing R which would mathematically represent the reputation of each peer, POR can main a list of trustworthy peers, which we can call them Transaction Validators. These Transaction Validators will be rewarded for their contribution to the system by providing computing power or storage capabilities.

The POR utilize directed acyclic graph on the basis of the social graph. The POR can tolerate Byzantine failures. As part of BITCONCH protocol, POR can help BITCONCH to scale: the greater the number of peers, the greater the TPS. POR is a perfect candidate for high-frequency small micro-transactions and DApp with social applications. POR adopts the power balance philosophy and designs a decentralized incentive system with anti-Matthew effect, which can ensure that new users and old users, small users and large users have the same opportunity to obtain system rewards. POR can prevent the system become centralized caused by ill-designed incentive mechanisms.

#### **3.1 Reputation And Consensus**

The ideal blockchain is a decentralized system with no central authority, such system will eliminate the potential threat of corruption and abuse caused by the concentration of power, as advocated by the blockchain pioneers such as CypherPunk, HashCash, and B-Money. The core of the blockchain technology is the consensus algorithm. The essence of the consensus algorithm is that in the distributed network, under the condition that each node does not trust each other, the Nash equilibrium is formed by the evidence of scarce resources, winning the trust of all parties, thus an agreement is achieved between the nodes and task will be completed synchronously.

For POW, the time and electricity consumed by the miners will be considered as

evidence, for POS or dPOS, the coins or coin-age will be considered as evidence. The consensus process is about to find someone who can be proved to hold a scarce resource as evidence and thus to be trusted to participate in the consensus process, contribute computing power, and receive rewards.

BITCONCH proposes that consensus can be reached by means of proof of reputation.

### **3.2 Reputation As Scarce Resource**

Traditionally, reputation can help the business community to evaluate the credibility of many potential trading counterparties, such as mortgage applicants, real estate renting applications, etc. On blockchain, reputation can help peers to decide who is trustworthy to participate in the consensus and who should get the reward for maintaining the system. Traditionally, reputation can be earned by paying back on time. On blockchain, reputation can be earned by maintaining the distributed ledger honestly and restrained from perpetrating malicious activities.

Reputation can be considered as a scarce resource, and in real life, reputation can be quantified as a rating ranks. On many e-commerce platforms such as Taobao or Amazon, users rely on centralized ratings from platforms (stars for Amazon or Diamonds/Crowns for Taobao) to decide which product to buy. In the investment market, users rely on centralized ratings from prestigious institutions such as Standard & Poor's and Moody's. When choosing a university, students use the reputation and ranking of the school to decide which one he or she should apply to. The accumulation of reputation requires time and effort, and the level of reputation and economic value also have a natural connection. As Buffett's famous saying, "It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently." Because of the scarcity and high value of reputation, using the reputation value as evidence can effectively reduce the possibility of malicious nodes.

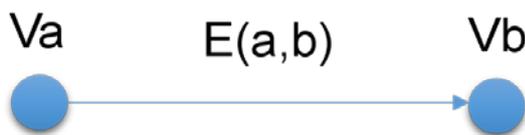
The BITCONCH chain uses a social graph and mathematical abstraction built by commercial activities to construct a quantifiable reputation system. It is fair for or anyone or an organization, hard to forge, and quantifiable. Anyone or organization can build and maintain its own reputation.

### 3.3 Math Model For Reputation

The social network can be mathematically abstracted and modeled, thus a Social Graph can be constructed. Everyone can be abstracted into points (Vertices/Node), and the relationship between people can be abstracted into one edge of the graph. We can use mathematical descriptions to describe the social relationships, intimacy, and personal credibility between people.

#### 3.3.1 Social Relationship

Assuming that a and b are two people, they can be represented as two vertices  $V_a$  and  $V_b$  in the figure. If a transaction occurred between a and b, a line can be drawn between vertices a and b, as  $E(a,b)$  which means the direction is from a to b. Also, We define the weight of  $E(a,b)$ , the amount and number of transactions can affect the weight value.



#### 3.3.2 Mutual Trust Node

For small micro-transactions, the mutual trust node (MTN) can open the "transaction channel" to perform high-frequency offline transactions. MTN can be formed in two ways: between friends and between high-reputation peers.

If there are a lot of transactions happening between two nodes, it can be inferred these two nodes (the people behind the nodes) would have a frequent social interaction, which means they are socially deep related. As illustrated by figure below, Jenny and Alice are friends, and they often interact through social Apps, such as: chatting through encrypted WeChat, photo sharing, money transfer (Red Packet or Transfer), leaving comments, etc. For people like Jenny and Alice, who are closely related in real life, with deep social relationships, we define them as "Friends or Relatives Nodes" (FRN). For FRN, the privilege of initializing high-frequency offline transactions is given.



Usually, two nodes without prior interactions cannot open payment channels. But for High-Reputation-Nodes, payment channel can be opened even without prior interactions. For High-Reputation-Nodes, since they have a good reputation performance in their own social networks. For small and microtransactions, being a malicious node is economically unfeasible, since the cost of reputation loss is far greater than the possible benefits.



### 3.3.3 Reputation Value Quantification

We define  $R$  which could represent the level of acceptance in a particular social group (or social network). On blockchain network, we build the reputation  $R$  from three dimensions: social activity  $D$ , time activity  $T$ , and contribution activity  $C$ . Thus we have the following equations:

$$\mathcal{R}(\alpha, \beta, t) = \omega_1 \mathcal{D}(E, t) + \omega_2 \mathcal{T}(S, t) + \omega_3 \mathcal{C}(N, t) \quad (1)$$

Where  $\omega_n$  is the weight, within a certain time  $t$ ,  $\mathcal{D}(\alpha, t)$  is the social activity of the node,  $\mathcal{T}(\beta, t)$  is the time activity of each node, and  $\mathcal{C}(\gamma, t)$  is the contribution activity. In order to make users being active continuously, and also to allow latecomers to participate in the system more fair, avoiding the Matthew effect brought by the first mover advantage (FMA), we specify that  $R$  will decays over time. The decay rate of  $R$  is defined as  $\mu$ , as shown in equation (2):

$$\mathcal{R}_n = \mathcal{R}_0 e^{\mu t} \quad (2)$$



Social activity D: It is determined by a number of factors such as the number of friends in the social network, the frequency of interaction with friends (ie, activeness), the reputation value of friends, and the amount of the transaction. The formula follows:

$$\mathcal{D}(E, t) = \sum_{i=1}^k \alpha E_i^{\beta \log(D_r)} \quad (3)$$

Where  $E_i$  is the weight function for each transaction.  $E_i$  is positively related to the transaction amount.  $D_r$  is the transaction object.  $\log(D_r)$  is a logarithmic function of the  $D_r$  reputation value.  $\log(D_r)$  is used to prevent a particular node generation high reputation by trading with mass amount of fake users.

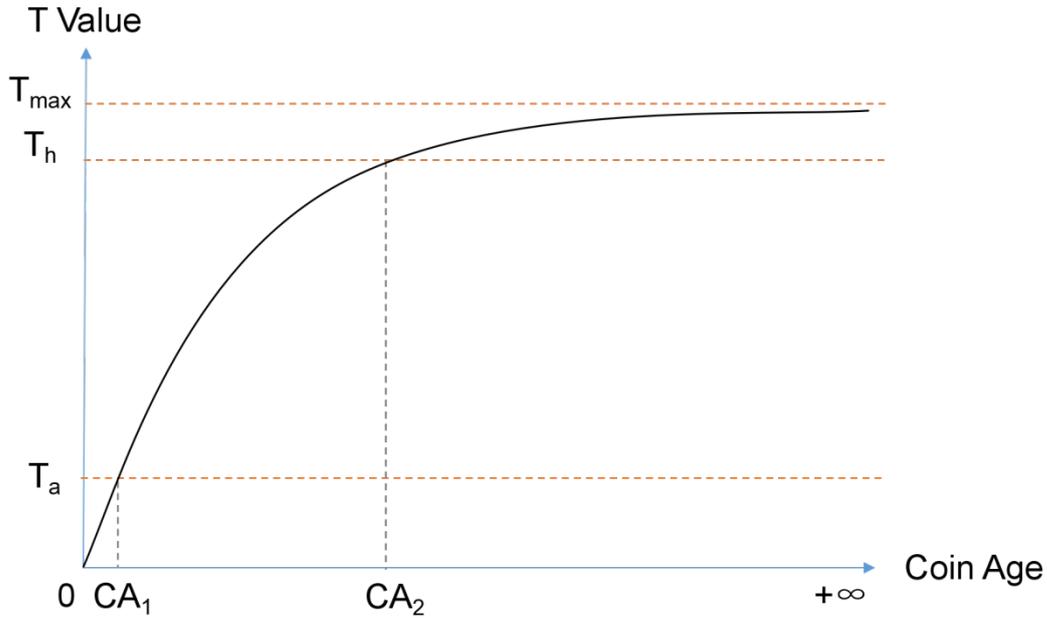
As shown in the figure: Tom has very few friends, and he barely communicates with his friends. On the other hand, Jack is very popular, not only he has a lot of friends, but also he frequently communicates with his friends, and some of his friends are high reputation nodes, and he formed mutual trust nodes with several of his friends. Jack can trade with friends via payment channel which is offline and instant. Then Jack's D value is much higher than Tom's D value.



-  Low Frequency, One Way
-  High Frequency, Interactive
-  Payment Channel
-  High Reputation Node

Time Activity T: This indicator is mainly determined by the coin-age of the BITCONCH held by the user. We believe that the long-term holders of BITCONCH are more credible than the non-holder and less likely to perpetrate malicious act. But unlike the PoS Consensus, money is not the only criterion for measuring whether a node is trustworthy or not. As shown in the figure, the logarithmic formula of  $T(\beta, t)$  provides a better chance for the majority of average users to obtain high credibility. The formula follows:

$$\mathcal{T}(S, t) = \beta + a \log(St) \quad (4)$$



Contribution activity C: This indicator  $C(\gamma, t)$  describes the level of contribution of a particular user did to the system, which indicates how much the node contributes to the system when the time is  $t$ , and  $N$  is the value of the Account Nonce, which is used to record the user's the frequency of contributions (storage or computing). The system will check the validity of the files by a time interval.

$$C(N, t) = \sum \alpha N_{file} + \beta \log N_{Rnd} \quad (5)$$

### 3.4 Consensus Process

The consensus process of POR is divided into two parts:

- (1) Defining a list of Transaction Validators
- (2) Verifying the transaction through the Byzantine-Fault-Tolerant process

Define Transaction Validator. In the blockchain network, there are  $N$  users, each user has a reputation value  $R$ . According to the reputation  $R$  of each node,  $n$  nodes with high  $R$  will be selected as List  $L$ .

There are two kinds of Transaction Validators: full node candidates and light node candidates.

Full-node users may come from commercial developers or other community the BITCONCH ecosystem. Since light nodes can run on devices such as smartphones and

home computers, almost all users can become light node candidates. The way in which all nodes and light nodes are jointly contributing cannot only stimulate the enthusiasm of both commercial developers and ordinary users but also curb the possible centralization tendency.

The Transaction Validators in  $\mathbb{L}$  verifies new transactions in the network through the Byzantine-Fault-Tolerant process. Successfully verified transactions are recorded in the system's distributed ledger while increasing the reputation value of the corresponding node. The Byzantine fault-tolerant process can still provide security and activity guarantees for the system when a limited malicious node exists.

### 3.5 Transaction Validators

The Transaction Validators in the list of  $\mathbb{L}$  take turns to participate in the verification process. Each round runs a Byzantine fault-tolerant protocol to verify the newly generated transaction. If all nodes in  $\mathbb{L}$  agree, the transaction is confirmed.

$\mathbb{L}$  is selected according to the current  $\mathcal{R}$  value of each node and a distribution function  $\mathbb{D}$ . For node  $x$ , the higher his  $R_x$ , the easier it is to be recorded in  $\mathbb{L}$ .

The probability of a node being selected into  $\mathbb{L}$  by  $\mathbb{P}$  is as follows:

$$\forall \alpha, \beta \in \mathbb{N}: \mathcal{R}(\alpha) \geq \mathcal{R}(\beta) \implies \mathbb{P}(\alpha|\mathbb{D}) \geq \mathbb{P}(\beta|\mathbb{D}) \quad (6)$$

Sort all nodes based on  $\mathcal{R}$  in a descending order.

Based on  $\mathbb{D}$ ,  $m$  random numbers are generated in  $[0, N)$ , and then taking the floor of all of them, we receive the selected nodes. In order to avoid double selection we select the closest yet unselected nodes with a higher reputation. If such node does not exist, then we do the same going towards the lower reputed nodes.

The distribution function  $\mathbb{D}$  would be an exponential function since exponential gives priority to the highly reputed nodes and can strongly suppress the lower ranked ones, depending on its variance.

### 3.6 Byzantine-Fault-Tolerance Process

After obtaining  $\mathbb{L}$ , the POR verifies the correctness of the transaction and updates the ledger through a Byzantine fault-tolerant process. We make the following definitions:

#### **NON-FAULTY-NODES :**

Nodes that are functioning correctly without error, obeying rules.

#### **FAULTY-NODES :**

The node with the error, including timeout, data corruption, and malicious behavior (Byzantine error).

We set the following preliminaries:

- The node uses 1 or 0 to indicate the transaction verification result. 0 is the verification success, 1 is the verification failure.
- All honest nodes make decisions within a limited time.
- All honest nodes make the same decision.

The reputation proves that the consensus is divided into several cycles, each cycle has several rounds, and each round will validate several transaction data, so  $\mathbb{L}(k)$  can be defined as the list of Transaction Validator in the  $k$ th round.

#### Consensus Process :

- Last rounds ended
- There are several unconfirmed transaction Tx0
- There are several new transactions Tx1 generated this round.
- Tx0 and Tx1 are combined into a transaction list Tx to be verified.
- Tx will be broadcast to all the nodes in  $\mathbb{L}(k)$ , the node in  $\mathbb{L}(k)$  will verify the transaction, and if the transaction gets enough node verification, the transaction will be updated to the ledger.
- If the malicious nodes of  $\mathbb{L}(k)$  is less than  $m/3$ , then the round is defined as success. The contribution activity of the nodes in  $\mathbb{L}(k)$  increases, and the transaction activity of the corresponding nodes increases.

### 3.7 Data Structure And Transaction Relationship

The BITCONCH uses DAG directed acyclic graph. As shown in Figure 1(a), Tx0 is the Genesis transaction, that is, the first transaction of the entire network and the initial users are assigned BITCONCH by a special address. Tx1, Tx2, Tx3, Tx4, Tx5, Tx6, ..., Txn are subsequent transactions. Because each transaction has a time (Time) and an order (Order), the entire transaction history can be represented as a directed acyclic graph.

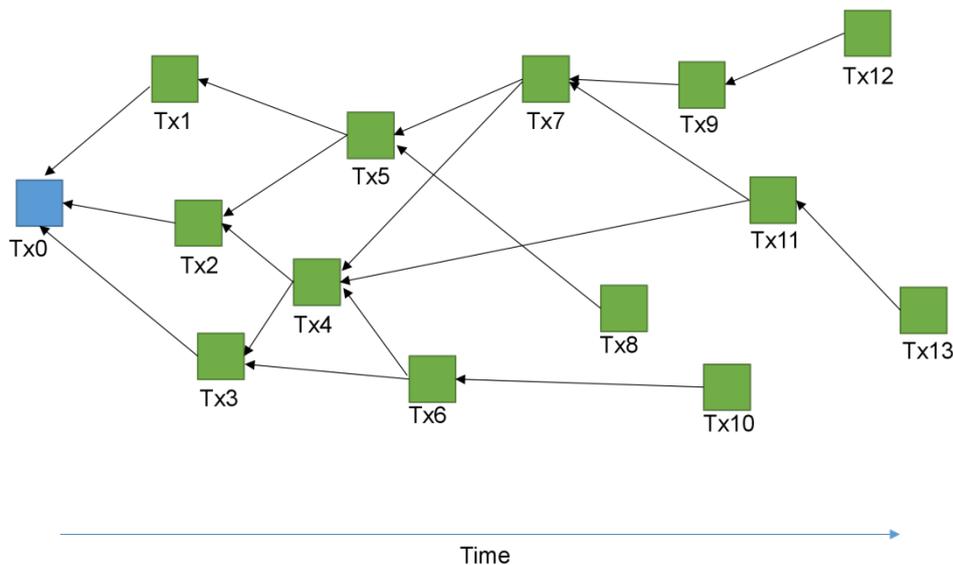


Figure 1 ( a ) DAG Data Structure

Tx0 is a transaction record for recharging node N1, corresponding to the first user N1 in Figure 1(b). Tx1 is the second transaction  $N1 \rightarrow N2$ , that is, N1 transfers some BITCONCHs to N2, and users N1 to N2 in the social graph will add an edge, that is, N1 and N2 begin to establish a social relationship. As the number of transactions Tx increases, there will be more and more edges between the nodes in the social graph, and the social network tends to mature.

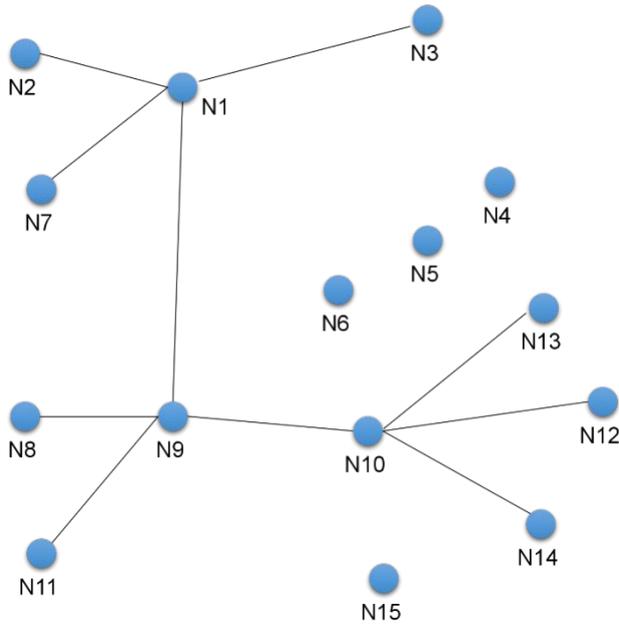


Figure 1 ( b ) Social Graph

Figures 1(a) and 1(b) show the interaction between the DAG data structure and the social graph. Fifteen users generated 14 transactions from Tx0, Tx1 to Tx13, and built a social relationship as shown in (b).

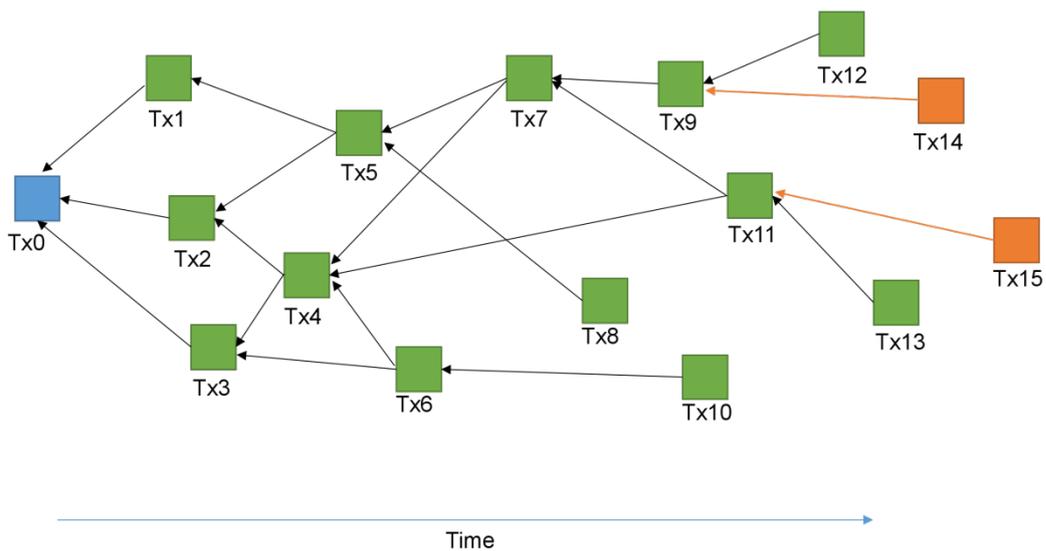


Figure 2 ( a ) New Transaction and Verification

As shown in Figure 2(a), new transactions Tx14 and Tx15 are generated. Where Tx14

indicates that N1 transfers n BITCONCHs to N4, and Tx15 indicates that N5 transfers n BITCONCHs to N1. If  $m > n$ , according to formula (3), the transaction amount is positively correlated with E value, for Reputation contribution, the weight of Tx14 is greater than Tx15. As transactions continue to increase, the links between the various nodes in the social graph continue to increase, providing more social data to feed reputation values.

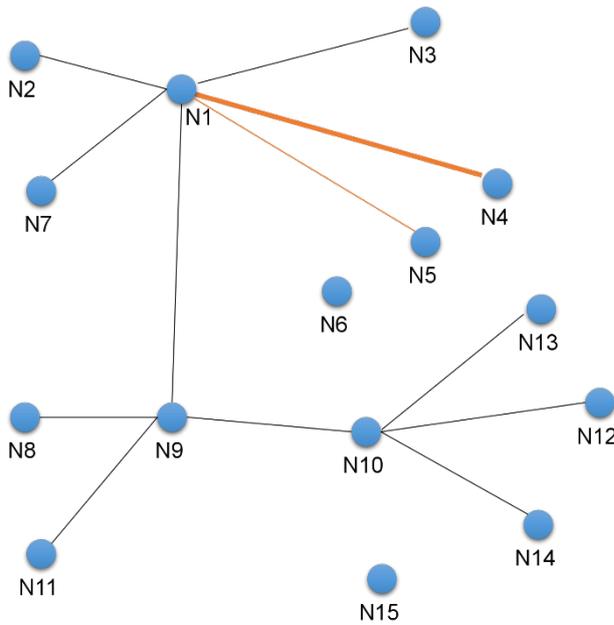


Figure 2 ( b ) New Transaction and Social Graph

Figure 2(a) also demonstrates the ability of the system to handle concurrent transactions. When Tx14 and Tx15 are generated simultaneously, the system can concurrently generate multiple Byzantine fault-tolerant processes to improve the efficiency of transaction verification.

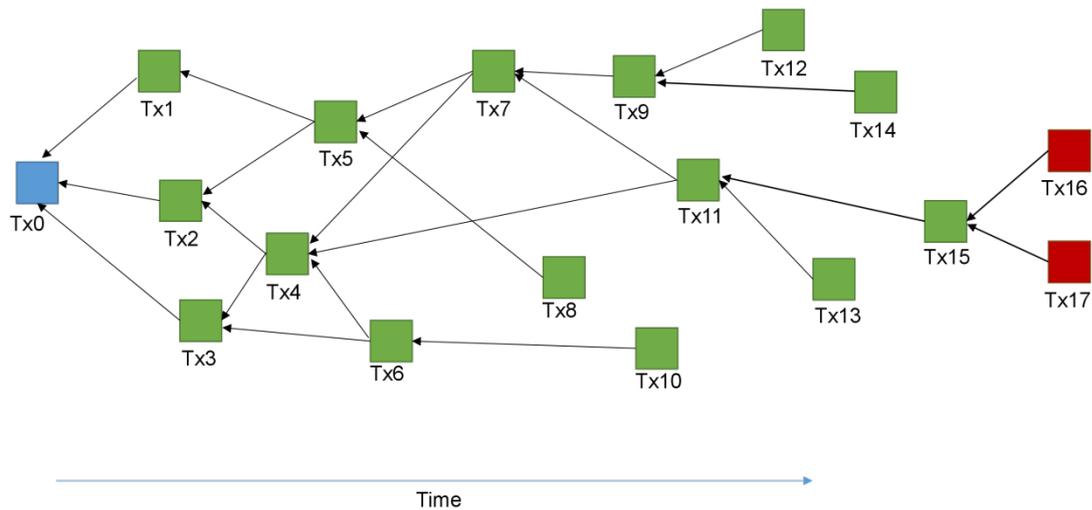


Figure 3 Double Spending

As shown in Figure 3, if the system has double-spending transaction Tx16 and Tx17 (N1 is a malicious node), due to the deterministic nature of the Byzantine fault tolerance process, even if Tx16 and Tx17 are simultaneously confirmed, when one of them is updated to the ledger, the other will be discarded due to insufficient balance, thus avoiding the occurrence of double-spending attacks. The malicious N1 node will be traced back and received a penalty, the reputation value will be reduced, and the qualification of the Transaction Validator will be lost. Because the cost of N1 is much higher than the potential benefit, the motion for N1 to become a malicious node is extremely low.

### 3.8 System Incentive Of Por

All 50 billion BITCONCH coins will be generated without mining. 20% ( 10 billion BITCONCHs) will serve as the initial reward pool for the POR reputation consensus. All the nodes (full nodes and light nodes) will have the same opportunity to be selected to participate in the consensus and get rewards.

In addition to the 10 billion initial BITCONCHs, the reward pool will be continuously supplemented by the benefits of the business ecosystem, such as transaction fees, application development fees, and promotion revenue. A sustainable reward pool maintains the enthusiasm of the nodes and contributes to the sustainable and healthy

development of the ecosystem.

The BITCONCH chain consists of a full node and a light node, which are selected by the user according to their own equipment and interests. The full node and the light node will share the system rewards in a 3:2 ratio.

Users who hold the ERC20 BITCONCH tokens (a total of 1 billion issued) can be migrated to the mainnet via a 1:50 swap ratio, once the mainnet is live.

### **SUMMARY OF POR CONSENSUS RULES :**

1. The BITCONCH chain adopts the Ethereum-like account structure. Each user has an account, and the account records the BITCONCH balance and reputation value of each user.
2. The mutual trust node (MTN) users can open a payment channel for small micro-transaction to initialize offline high-speed transactions.
3. The honest nodes with trustworthiness are dynamically chosen by the R to form a list L of Transaction Validators.
4. The honest nodes can gain system reward by contributing computing power to maintain the integrity of the system.
5. Large amount transactions between mutually trusted nodes, and transactions between non-mutually trusted nodes are verified by the Transaction Validators.

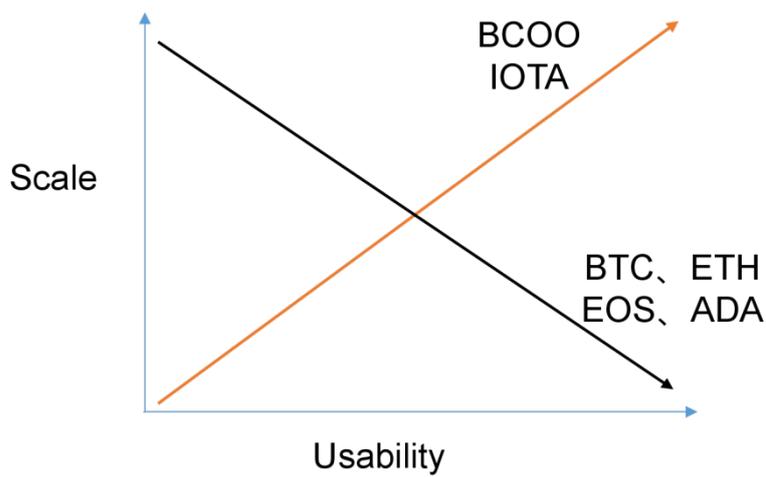
### 3.9 Comparison Of Por And Various Consensus Mechanisms

As can be seen from the comparison of the following table, the POR reputation consensus mechanism not only performs well in supporting high throughput and high concurrency, but also has positive scalability, and the more users, the faster the transaction speed. While maintaining a low usage fee, we will maintain the enthusiasm of the participation of the whole community through credit incentives and maintain the decentralization of the entire network.

Protocols	BTC	ETH	EOS	ADA (Cardano)	IOTA	BITCONC H
Consensus Algorithm	PoW	PoW	DPoS	Ouroboros	DAG+Tangle	PoR
Evidence	Time + Electricity	Time + Electricity	Coins(Stake)+Votes	Coins(Stake)	Time	Reputation
Default Penalty	Work is ignored, no rewards	Work is ignored, no rewards	Loss of qualification	Loss of qualification	Work is ignored, no rewards	Loss of qualification Reputation Damaged
Fault Tolerance	1/2 + 1	1/2 + 1	1/3 + 1	1/2 + 1	1/3+1	1/5 + 1
Throughput	3~7	5~20	1,000	257	800	10,000+
High concurrency	No	No	Yes	Yes	Yes	Yes
Decentralization	Mining Pool	Mining Pool	Super Node (or Block Producers)	Players with loads of Coins	Decentralized	Decentralized

Transaction Cost	High	High	Low	Low	Low	Low
Enthusiasm	High	High	High but only for block producers	Low	Low	High, All players will participate in the consensus process, and get rewarded.

### Scalability



## **4. Other Breakthrough**

### **4.1 Zero-Knowledge-Proof**

BITCONCH protects user privacy by encrypting transaction details with zero-knowledge proof-technology. Traditional blockchains, such as Bitcoin and Ethereum, distribute large-scale ledger data across untrusted network nodes, and the information stored on the chain is completely public. Even if the user uses the new address each time, the attacker can still determine the user's true identity by analyzing the user's habits, spending amount, transaction time and other information.

Zero-Knowledge-Proof protects user privacy by encrypting transaction details. Zero-knowledge verification uses a ZKP architecture in which a prover can prove to a verifier that he or she has some kind of information (such as a private key in an encryption key) without revealing the content of the information.

### **4.2 Thin Client**

Clients of traditional blockchains(Bitcoin or Ethereum), would grow larger and larger as network nodes number increases, slower speeds, and higher costs, which are beyond the reach of average users. Inevitably, most ordinary people are difficult to participate in the system process, and resources and computing power are more concentrated in the hands of a few participants, forming the Matthew effect.

The BITCONCH chain achieves lightweight of nodes through both Snapshot and distributed hash tables(DHT). Simplified light nodes that can run on low-config-devices, including smartphones, home computers, etc., participate in system billing. Tens of millions of light nodes are good for combating centralization and ensuring the decentralized nature of the system.

### **4.3 Smart Contract And Fork Management**

BITCONCH will provide dev toolkit , which will allow community developers to generate modifiable smart contract templates. Based on the templates and rules provided by BITCONCH, users can develop smart contracts that are easy to upgrade and manage. Due to the philosophy that blockchain data cannot be changed, any modification will result for potential forks, so for smart contracts or similar changes with significant stakes, BITCONCH uses a voting scheme. The stakeholder will vote with its own Stake at a certain time, to ensure a consensus among the communities.

### **4.4 Quantum-Proof Encryption Algorithm**

Asymmetric encryption algorithms (Asymmetrical), such as ECC256, SHA256, SHA3, etc., are used in traditional blockchains such as Bitcoin and Ethereum. These encryption algorithms are easily cracked by quantum computers.

Cryptographic systems currently considered to be resistant to quantum attacks include hash cryptosystems, coded cryptosystems, lattice cryptosystems, multivariate secondary cryptosystems, and key cryptosystems. This cryptosystem s can resist both classic and quantum attacks while the key length is long enough. In order to cope with the coming of the quantum computer era, BITCONCH will adopt cryptographic algorithms against quantum attacks.

### **4.5 Bvm And Programming Language**

BITCONCH Chain enriches the BITCONCH ecosystem by providing a variety of tools to enable developers to build their own distributed applications. The BITCONCH chain provides a solidity-based programming language BO and a corresponding virtual machine BVM, as shown in the figure. On the BITCONCH chain, developers translate business logic into smart contracts through programming languages, and smart contracts will be compiled into bytecodes that machines can run through virtual machines.

BVM has three major advantages over EVM:

### **1. Using BVM makes it easier to develop powerful smart contracts.**

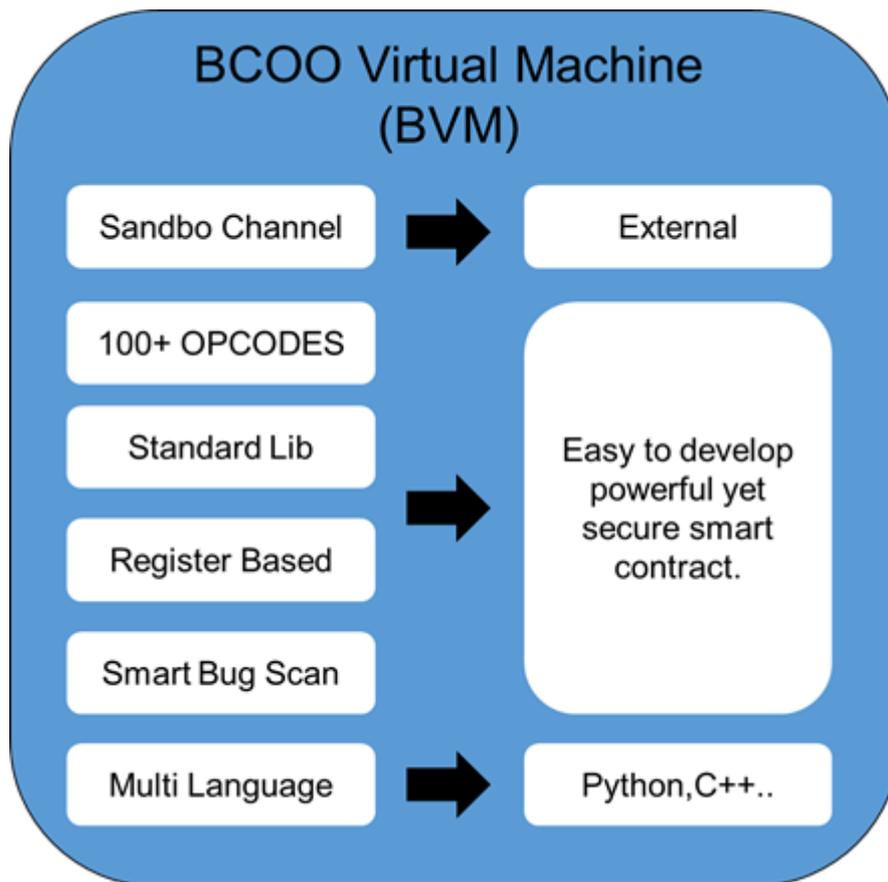
Compared to Ethereum's 65 opcodes, Baker Chain will provide more optional opcodes and standard libraries for developers to develop more high-quality DApps, extending the functionality of more social and landing applications. Because there are usually a lot of tokens in smart contracts, once an error occurs, it will cause huge losses to developers and users, so BVM will provide smart tools to detect transaction order, time stamp, accident handling and reentrant vulnerability (Reentrancy Vulnerability) and other common bugs. To increase development speed and make it easier for developers to write smart contracts, BVM will be a register-based virtual machine.

### **2. BVM provides an interface to enable smart contracts to communicate with the outside world.**

Relative to the sandbox environment of EVM and external world isolation (unable to use the permissions of the network, files or other processes), BVM establishes a transmission channel through digital signatures to solve the communication problems between smart contracts and the outside world.

### **3. Support multi-language development**

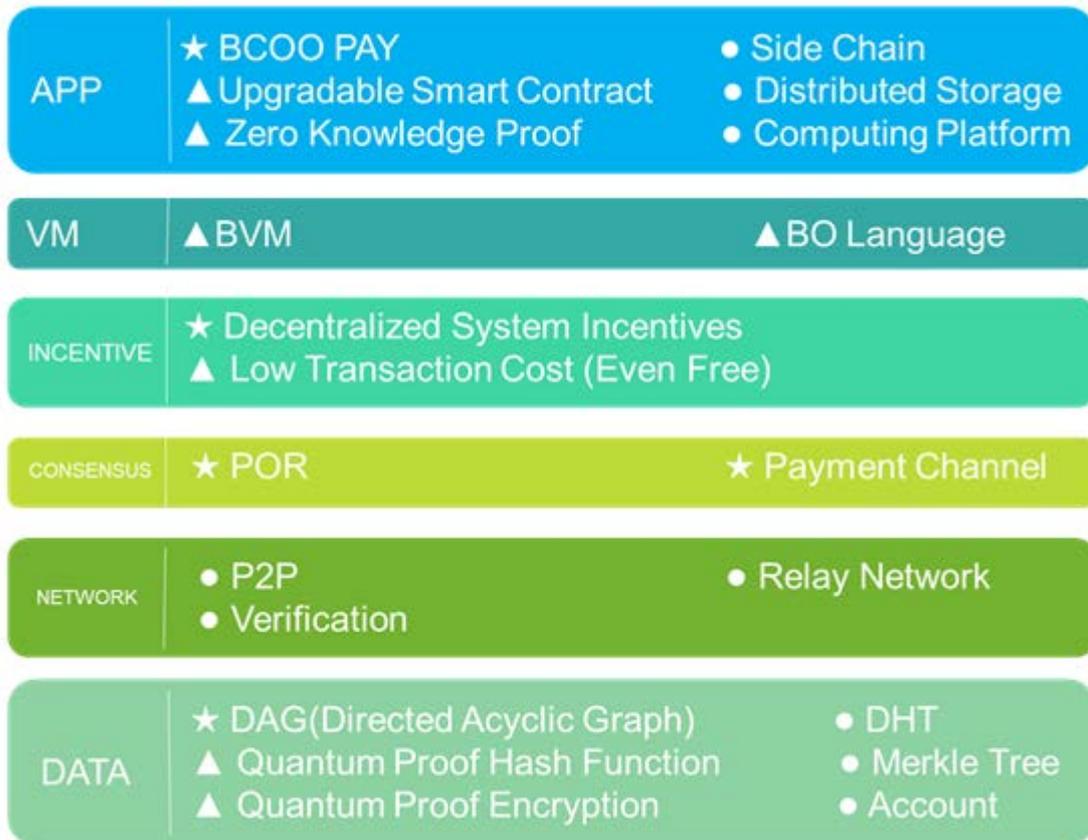
In order to allow more developers to join the BITCONCH community, BVM will support Python, Java, C++ and other development languages in the future.



#### 4.6 Side Chain

The BITCONCH chain supports different hooking mechanisms (Two-way Pegging) to achieve the union of the main chain and the side chain. BITCONCH will provide developers with sidechain development templates. In the future application scenario, BITCONCH as the main chain will mainly provide trusted accounting and reputation management, and more diverse and colorful commercial functions will be open to the community to develop on their own side chains. For example, BITCONCH Chain will provide distributed storage capabilities, and developers can implement file storage, multimedia and other functions on their own sidechains.

## 5. System Architecture Diagram



Note:

The ▲ item is based on the most advanced technology or algorithm currently used;

★The item is a technology or algorithm that has independent Intellectual innovation and core competitiveness.



## **6. Real-World-Application Scenario Outlook**

### **6.1 Bitconch Pay**

Currently, BITCONCH PAY is developed and operated by the BITCONCH R&D team and has been launched on IOS and Android. BITCONCH PAY integrates key functions such as key management, smart payment, and an entry point for a local business application or other commercial apps. In the future, after the BITCONCH main net is live, BITCONCH PAY will become the BITCONCH light node client.

### **6.2 Other Possible Applications And Technical Support**

BITCONCH Chain provides developers with a friendly sidechain and DApp development environment. The BITCONCH Foundation will also provide technical support and project incubation services for important social applications to help users quickly build social graphs and personal reputation through more application products. The following table lists some of the foreseeable and predictable applications and analyzes and compares the technical requirements of the product itself and the technical support that BITCONCH can provide.

TYPE	REQUIREMENT							
	SOCIAL GRAPH CONTRIBUTION	HIGH THROUGHPUT	HIGH CONCURRENCY	FILE STORAGE	LOW TRANSACTION COST	PRIVACY	BUSINESS REPUTATION	FREQUENT ITERATION
DChat	▲▲▲	★★	★★	★	★★★★	★★★★	★	★★
Social Media	▲▲	★★	★★	★★	★★	★★	★★	★
eCommerce	▲▲▲	★★★★	★★★★	★★	★	★	★★★★	★
Video/Streaming	▲	★★	★★	★★★★	★★	★	★	★
Video GaaS	▲	★★★★	★★★★	★★★★	★	★	★	★★★★
Fin-Tech	▲▲▲	★	★	★	★	★★★★	★★★★	★
Crowd-Funding	▲▲	★★	★★	★★	★	★	★★★★	★
Shared Economy	▲▲	★★	★★	★★	★	★★	★★★★	★

▲ : Represents the extent to which the application can contribute to the BCO Chain POR Consensus. The greater the number of triangles, the greater the contribution.

★ : Representing the importance of the application to a particular demand, the more pentagrams, the higher the demand.

The interaction between the BITCONCH main network and the side chain is shown in Figure 4. Most of the commercial applications may run on the side chain, transaction information is recorded on the main network, and the reputation data is fed to the main network. While each application comes with its own traffic, there is an inevitable interaction between users (see Figure 5), which outlines a richer social graph and ecosystem. Commercial application developers can accumulate higher reputation since they have more social connections and frequent transactions. The higher the reputation, the higher the probability of being selected as the “Transaction Validators”, the more system rewards are obtained.

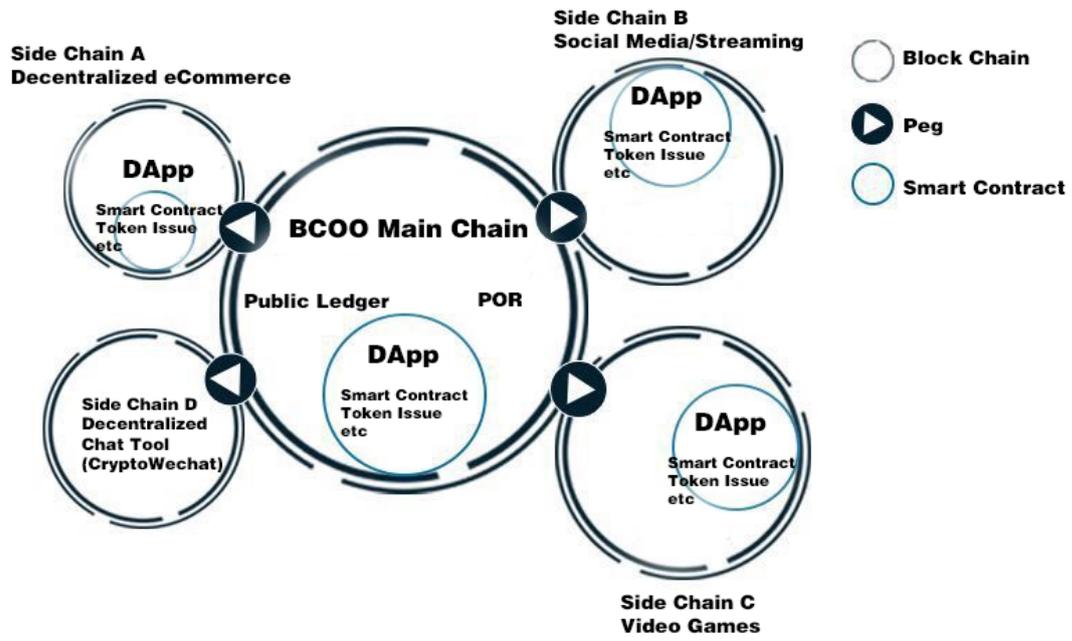


Figure 4. Interaction diagram between BITCONCH main network and side chain

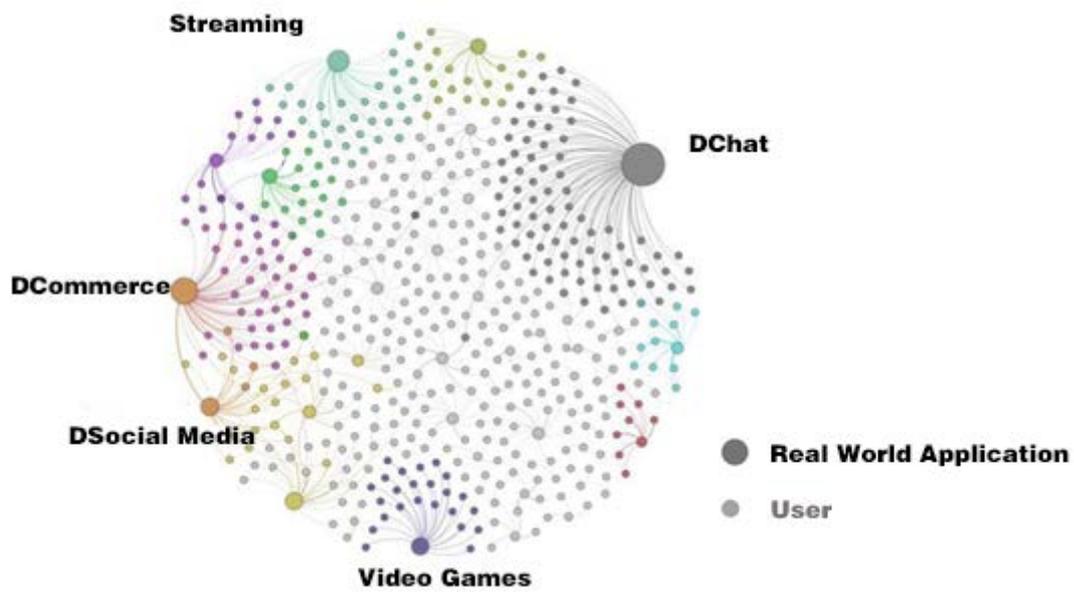


Figure 5. Traffic Sharing that may exist between applications

## 7.Conclusion

BITCONCH chain innovatively proposed the POR reputation consensus algorithm, the decentralized reputation system and incentive mechanism based on the social graph, and respectively met the large-scale commercial application requirements through the following technologies, especially high-frequency micro-transaction and social Apply technical requirements in terms of scalability, security, and dispersion. The BITCONCH chain aims to establish a decentralized distributed blockchain underlying public chain and business ecosystem that can serve tens of millions of users.

BUSINESS APPLICATION TECHNOLOGY REQUIREMENT	RELATED TECHNOLOGIES USED BY BITCONCH CHAIN	THE GOAL THAT THE BITCONCH IS TRYING TO ACHIEVE
High concurrent high throughput	POR Social Graph	10,000+ TPS And the more nodes, the faster the network, the safer the network
Keep decentralized	Light client	Light client can run on smartphone
Large file storage	Lattice fragment storage	In principle, there is no storage limit
Low transaction cost	POR	Zero Cost Transactions
Effective incentive of the node	Reputation incentive system	High-reputation users follow the rules to get rich rewards, and if users perpetrate malicious act , they will have to pay a very high price.
Privacy	POR Zero-Knowledge-Proof	User information encryption protection Business behavior can be easily defended
Friendly development environment	Side Chain Support JavaScript/Solidity Support	Suitable for high frequency micropayment applications and social products
Upgradable Smart Contract	ROR and Stake Voting Scheme	Quick and efficient product iteration and bug fixes

## 8. References

1. Nick Szabo. Formalizing and securing relationships on public networks. First Monday, 2(9), 1997
2. Back, "Hashcash - a denial of service counter-measure," <http://www.hashcash.org/papers/hashcash.pdf>. 2002
3. Vitalik Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2013
4. Gavin Wood. Ethereum: A Secure Decentralized Generalised Transaction Ledger. 2018
5. W. Dai, "b-money," <http://www.weidai.com/bmoney.txt>. 1998
6. Andreas Antonopoulos : Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 2014
7. Sheldon M. Ross. A First Course in Probability. 2009
8. Nash John. "Non-Cooperative Games" The Annals of Mathematics. 1951
9. Schlegel, H.: Reputation Currencies. Institute of Customer Experience.
10. Marko Vukolić: The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. 2016
11. Adam Back, Matt Corallo : Enabling blockchain innovations with pegged sidechains
12. Vitalik Buterin : Zk-SNARKs: Under the Hood
13. Eli Ben-Sasson : Zerocash: Decentralized Anonymous Payments from Bitcoin
14. Petar Maymounkov : Kademlia: A Peer-to-Peer Information System Based on the XOR Metric
15. Everett Hildenbrandt : VM: A Complete Semantics of the Ethereum Virtual Machine
16. L. LamPoRt, Constructing digital signatures from a one-way function, Technical RePoRt SRI-CSL-98, SRI International Computer Science Laboratory, Oct. 1979.

17. "Winternitz one-time signature scheme"

<https://gist.github.com/karlgluck/8412807#comment-1258433>