Bitconch Chain, A Newly Distributed Web Protocol Based on an Innovative Proof of Reputation (PoR) Consensus Algorithm and Eco System

Chen Zhiying, Liu Qiang, Joseph Sadove, Liu Gang*

Bitconch blockchain technology corp. Shanghai, 200040 China

*Corresponding Author email: gangliuleon@gmail.com

Keywords: Negotiation algorithm; ecosystem; Web protocol; Bitconch chain

Abstract: Bitconch chain proposed an innovative POR (Proof of Reputation) reputation consensus algorithm, which offers a new solution that leverage blockchain technology to maintain both high throughput and decentralization. According to social graphs, Bitconch blockchain mathematically models social network, time, and contribution activities to build a decentralized reputation system, which offer a chance to transform the above items into every single user' reputation value. The higher the user's reputation, the lower the transaction cost (or even free of charge), and also has more opportunities to be selected as trust nodes to participate in the consensus and win better benefits. Users with high-reputation are defined as "Mutual Trust Nodes", who can start "payment channels" for high-speed offline transactions through micro-transactions.

1. Introduction

The birth of Bitcoin has made blockchain technology leap from pure theoretical research to the world's focal point of innovation and technology. Blockchain technology has initiated new ways to understand security and information usage and is now widely viewed as certain to dramatically change the world. The success of Ethereum and its Solidity language has permitted creation of Turing-complete smart contracts and allowed developers to create any kind of application to run on a blockchain. However, the Merkle-tree architectures used by Ethereum, Bitcoin and others suffer from several limitations and these are what is holding them back from large-scale commercial adoption.

2. The Challenge of Blockchain in Applications

2.1 High Concurrency, High Throughput and Scalability

The core of business competition is volume competition. A successful business project will have more than 10 million registered users and more than one million active users. Merkle-tree based blockchain architectures are severely limited in the speed and volume of transactions that can be processed. They are inherently not scalable without sacrificing their decentralization or security features. The fairly recent recognition of this has led to a burst of activity by these types of architectures (most notably Ethereum) to try to overcome these issues. In the commercial world, the ability to support system throughput in the range of tens of thousands of transactions per second –the current volume and speed Visa/MasterCard support – is expected of any potential replacement technology.

2.2 Incentive Mechanism and Transaction Costs

The business application scenario is mainly for high-frequency small and micro-transactions for a range 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.

  DOI: 10.25236/systca.18.083

2.3 Security and Decentralization

In order to ensure transaction security, the clients need to download and backup all the transaction data of the whole network, these clients are 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 micro-transactions, and have no ability or demand to purchase large computers and bear the corresponding operating costs. Therefore, small 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 and potentially compromising the consensus mechanisms supporting security.

3. Proof of Reputation Consensus Algorithm

3.1 Reputation and Consensus

As advocated by the blockchain pioneers such as CypherPunk, HashCash, and B-Money, the ideal blockchain is a decentralized system, a system with no central authority. An ideally decentralized system eliminates the potential threat of corruption and abuse caused by the concentration of control. The core of much of the blockchain technology is the consensus algorithm. The essence of the consensus algorithm is that in a distributed network and 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 among the nodes and permit the task to will be completed synchronously.

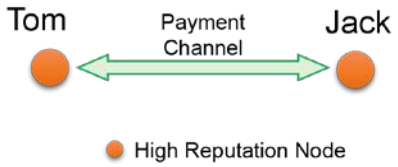
3.2 Reputation as Scare Resource

The business community relies on reputation and reputation markers to help evaluate the trustworthiness and creditworthiness of many potential counterparties, such as mortgage applicants and other loan transactions, trading financing, etc. On a 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. Reputation in existing business environment 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.

3.3 Mathematical Model for Reputation

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

Usually, 2 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 micro- transactions, being a malicious node is economically unfeasible, since the cost of reputation loss is far greater than the possible benefits.



3.4 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 is the weight, within a certain time t, D(α, t) is the social activity of the node, T(β, t) is the time activity of each node, and C(γ, t) is the contribution activity. In order to keep users continuously active and allow latecomers to participate in the system more fair while 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 μ, as shown in equation (2):

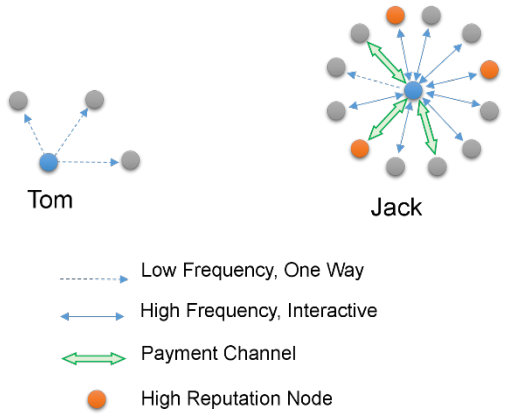
$$\mathcal{R}_n = \mathcal{R}_0 e^{\mu t} \tag{2}$$

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:

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

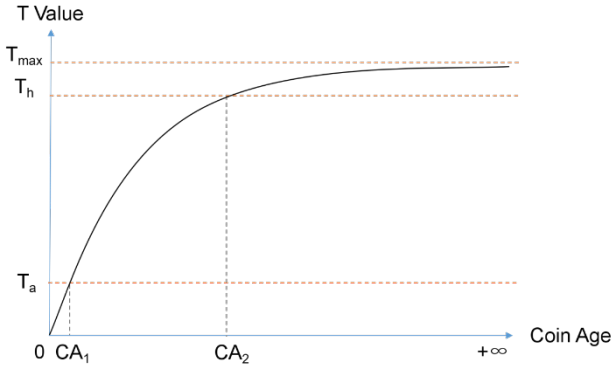
Where E_i is the weight function of each transaction. E_i is positively related to the transaction amount. D_r is the transaction object. $\log(D_r)$ is a logarithmic function of the D_r reputation value. $\log(D_r)$is used to prevent a paritular node generation high reputation by trading with mass amount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

As shown in the figure: Tom has very few friends, and he barely communicates with them. On the other hand, Jack is very popular, not only he has a lot of connectors, but also communicate very frequently, 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.



Time Activity T: This indicator is mainly determined by the coin-age of the Bus held by the user. We believe that the long-term holders of Bus 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(β,t) provides a better chance for the majority of average users to obtain high credibility. The formula follows:

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



Contribution activity C: This indicator C(γ, 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.

$$\mathcal{C}(N,t) = \sum \alpha \mathrm{N}_{file} + \beta \log \mathrm{N}_{Rnd} \tag{5}$$

3.5 Date Structure and Transaction Relationship

The Bitconch uses DAG directed acyclic graph. As shown in Figure 1, Tx0 is the Genesis transaction, that is, the first transaction of the entire network and the initial users are assigned Bus 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.

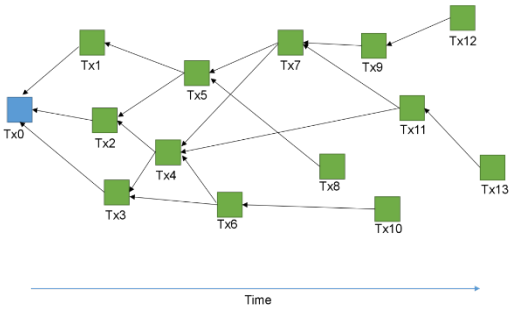


Fig 1 DAG Data Structure

Tx0 is a transaction record for recharging node N1, corresponding to the first user N1 in Figure 2. Tx1 is the second transaction N1N2, that is, N1 transfers some Buses 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.

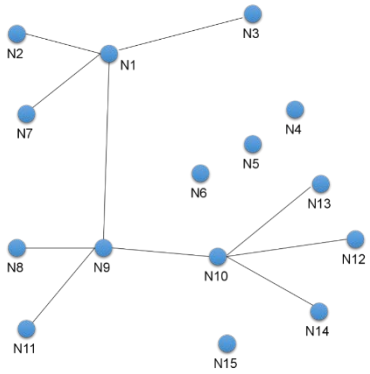


Fig 2 Social Graph

Figures 1and 2 show the interaction between the DAG data structure and the social graph. 15 users generated 14 transactions from Tx0, Tx1 to Tx13, and built a social relationship as shown in 2.

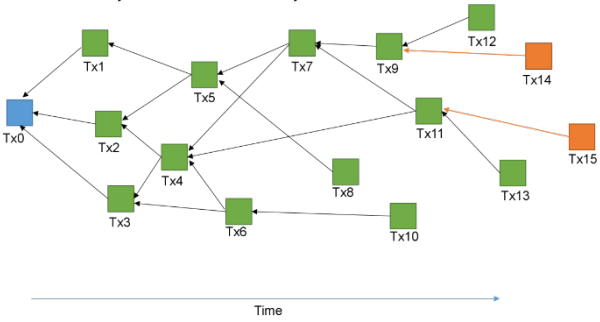


Fig 3 New Transaction and Verification

As shown in Figure 3, new transactions Tx14 and Tx15 are generated. Where Tx14 indicates that

N1 transfers n Buses to N4, and Tx15 indicates that N5 transfers n Buses 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.

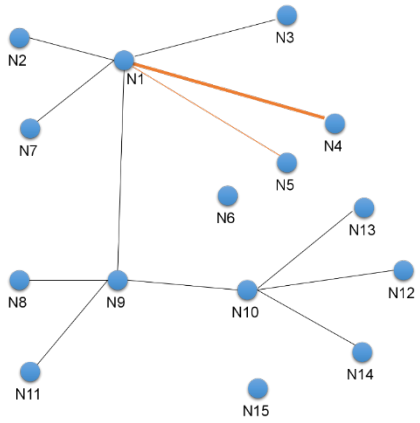


Fig 4 New Transaction and Social Graph

Figure 3 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.

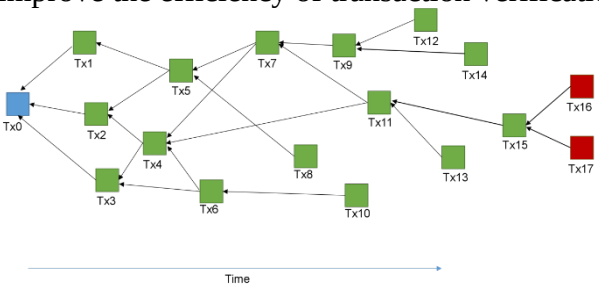


Fig 5 Double Spending

As shown in Figure 5, 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.

4. Other Breakthrough

4.1 Zero-Knowledge-Proof

Bitconch protects user privacy by encrypting transaction details with zero-knowledge proof-technology. Existing blockchain, 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 used 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.

4.2 Thin Client

Clients of existing 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.

4.3 Smart Contract and Fork Management

Bitconch will provide dev tool kit, which will allows 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.

5. Conclusion

Bitconch has proposed the innovation of the POR reputation consensus algorithm, the decentralized reputation system and incentive mechanism based on the social graph. This innovation meets the large-scale commercial application requirements through application the techniques, features and technologies itemized below. The platform's solution set is particularly supportive of high-frequency micro-transaction and social networks and assures scalability, security and decentralization.

References

[1] Graham A L , Cha S , Papandonatos G D , et al. Improving adherence to web-based cessation programs: a randomized controlled trial study protocol.[J]. Trials, 2013, 14(1):1-15.

[2] Van D D S , Elske S , Filip S , et al. Web-based cognitive bias modification for problem drinkers: protocol of a randomised controlled trial with a 2x2x2 factorial design[J]. Bmc Public Health, 2013, 13(1):674-674.

[3] Nadine Köhle, Drossaert C H , Schreurs K M , et al. A web-based self-help intervention for partners of cancer patients based on Acceptance and Commitment Therapy: a protocol of a randomized controlled trial[J]. Bmc Public Health, 2015, 15(1):1-13.

[4] Adolfsson A , Linden K , Sparudlundin C , et al. A web-based support for pregnant women and new mothers with type 1 diabetes mellitus in Sweden (MODIAB-Web): study protocol for a randomized controlled trial.[J]. Trials, 2014, 15(1):1-7.

[5] Lobban F , Dodd A L , Dagnan D , et al. Feasibility and Acceptability of Web-based Enhanced Relapse Prevention for Bipolar Disorder (ERPonline): Trial Protocol.[J]. Contemporary Clinical Trials, 2015, 41:100-109.

[6] van Spijker B A , Calear A L , Batterham P J , et al. Reducing suicidal thoughts in the Australian general population through web-based self-help: study protocol for a randomized controlled trial.[J]. Trials, 2015, 16(1):1-10.

[7] The evaluation of an interactive web-based Pulmonary Rehabilitation programme: protocol for the WEB SPACE for COPD feasibility study[J]. Bmj Open, 2015, 5(8):97-109.

[8] Yuan Q , Liu S , Tang S , et al. Happy@Work: protocol for a web-based randomized controlled trial to improve mental well-being among an Asian working population[J]. Bmc Public Health, 2014, 14(1):1-9.

[9] Leu J S , Hsu K C , Song T . Enhancing the Presence Service Efficiency of Internet Protocol Multimedia Subsystem-Based Web Services[J]. Wireless Personal Communications, 2015, 85(4):2319-2331.

[10] Santos E T P , Fialho S V . A Web-based tutor for Internet communication protocols[J]. Computer Applications in Engineering Education, 2010, 8(3-4):150-156.