BCAC: New Retail Ecology Based on Blockchain

Yellow Paper

BCAC Consensus Team

Abstraction: This paper presents the preliminary design and technical details of the BCAC new retail ecosystem. Includes authentication mechanisms for users and billing nodes, improved DPOS mechanisms for elections for ledger nodes, RAFT+ consensus algorithms, and side chain technologies.

1. Background

It appears block chain technology, provides a great driving force for the various industries to solve the problem transactions and consensus. However, with the in-depth development of the blockchain application, the blockchain has a long-standing problem, which limits the practical application of the blockchain. For example, the performance of bitcoin, ethereum, pseudo decentralization of eos, and so on. From the design point of view, the public chain as a transaction settlement chain is not suitable and should not bear the demand for application data winding.

But in the short term, there will be no new generation of digital currency that will replace bitcoin and ethereum as the basis of digital currency. And as an ecological, block chain and digital assets should not be competing with each other and substituted relationship. In the design of BCAC, the entire blockchain technology will serve as an ecology, and the application data will be stripped from the basic public chain through the sidechain technology. Reduce the pressure on the grassroots public chain data / settlement, while supporting the blockchain application, especially the new retail blockchain application through high-performance blockchain technology.

1. Authentication
   1. KYC

Know Your Customer (KYC) is the process of a business identifying and verifying the identity of its clients. The significance of “Know Your Customer” (KYC) is becoming increasingly important.

“KYC” refers to the steps taken by a financial institution (or business) to:

Establish the identity of the customer

Understand the nature of the customer’s activities (the primary goal is to verify that the source of the customer’s funds is legitimate)

Assess money laundering risks associated with that customer for purposes of monitoring the customer’s activities

* 1. BCA

Business Credit Authentication（BCA）is the process of identifying and verifying the identity of business partner, ledger node owner. “BCA” refers to:

Establish the identity of the customer

Understand the nature of the customer’s activities (the primary goal is to verify that the source of the customer’s funds is legitimate)

Assess money laundering risks associated with that customer for purposes of monitoring the customer’s activities

Assess business credit.

1. DPOS

Delegated Proof of Stake (DPOS) is the fastest, most efficient, most decentralized, and most flexible consensus model available. DPOS leverages the power of stakeholder approval voting to resolve consensus issues in a fair and democratic way. All network parameters, from fee schedules to block intervals and transaction sizes, can be tuned via elected delegates. Deterministic selection of block producers allows transactions to be confirmed in an average of just 1 second. Perhaps most importantly, the consensus protocol is designed to protect all participants against unwanted regulatory interference.

Under DPOS, the stakeholders can elect any number of witnesses to generate blocks. A block is a group of transactions which update the state of the database. Each account is allowed one vote per share per witness, a process known as approval voting. The top N witnesses by total approval are selected. The number (N) of witnesses is defined such that at least 50% of voting stakeholders believe there is sufficient decentralization. When stakeholders expresses their desired number of witnesses, they must also vote for at least that many witnesses. A stakeholder cannot vote for more decentralization than witnesses for which they actually cast votes.

Each time witnesses produce a block, they are paid for their services. Their pay rate is set by the stakeholders via their elected delegates (to be discussed later). If a witness fails to produce a block, then they are not paid, and may be voted out in the future.

The slate of active witnesses is updated once every maintenance interval (7 day) when the votes are tallied. The witnesses are then shuffled, and each witness is given a turn to produce a block at a fixed schedule of one block every 2 seconds. After all witnesses have had a turn, they are shuffled again. If a witness does not produce a block in their time slot, then that time slot is skipped, and the next witness produces the next block.

Anyone can monitor network health by observing the witness participation rate.

1. RAFT
   1. Consensus problem

In a distributed system, a consensus problem is that for a group of servers, given a set of operations, we need a protocol to finally agree on their results.

Because CAP theory tells us that for distributed systems, if we don't want to sacrifice consistency, we can only give up usability. Therefore, the data consistency model mainly has the following types: strong consistency, weak consistency, and final consistency. In the section, we mainly discuss the algorithm Raft, which is a strong consistency implementation algorithm in distributed systems.

The principle of general implementation of strong consistency: When one of the servers receives a set of instructions from the client, it must communicate with other servers to ensure that all servers receive the same instructions in the same order, so that all The server produces consistent results and looks like a machine.

Raft has several features:

Strong Leader: Raft uses a stronger form of leadership than other algorithms. For example, billing events are only sent from the leader to other servers. This simplifies the management of billing events, making Raft easier to understand.

Leader Selection: Raft uses a random timer to pick the leader. This approach only adds a little change to the heartbeat mechanism that all algorithms need to implement, making it easier and faster to resolve conflicts.

Membership Change: Raft uses a new joint consensus approach to adjusting membership in a cluster. Most of the differently configured machines in this approach overlap when converting relationships. This allows the cluster to continue to operate when the configuration changes.

* 1. Replicated State Machine

The consistency algorithm is proposed in the context of a replication state machine. In this method, the state machine on a set of servers produces a copy of the same state so that even if some servers crash, the set of servers can continue to execute. Replication state machines are used in distributed systems to solve many problems related to fault tolerance.

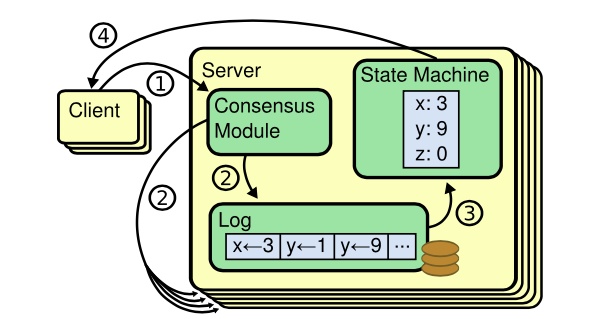


Figure-1: Architecture of the replication state machine.

The consistency algorithm manages the replication log from the client state commands. The order of the commands in the log processed by the state machine is the same, so the same execution result is obtained.

As shown in Figure-1, the replication state machine is implemented by copying logs. Each server holds a log containing a series of commands, and the state machine executes these commands in order. Because the state machine of each computer is deterministic, the state of each state machine is the same, the commands executed are the same, and the final execution result is the same.

How to ensure that the replication log is consistent is the work of the consistency algorithm. On a server, the consistency module accepts the client's commands and adds commands to its logs. It communicates with the coherency modules on other servers to ensure that each log eventually contains the same sequence of requests, even if some servers are down. Once these commands are properly copied, each server's state machine executes them in the same order and returns the results to the client. In the end, these servers look like a reliable state machine.

Consistency algorithms applied to actual systems generally have the following characteristics:

Ensuring security (never returning a false result), even in all non-Byzantine cases, including network latency, partitioning, packet loss, redundancy, and out of order.

High availability, this cluster is available as long as most of the machines in the cluster are operational, can communicate with each other and can communicate with the client. Therefore, in general, a cluster with 5 machines can tolerate the failure of 2 of them. When the server stops working, we think it has failed. Maybe it will recover from it when they have stable storage and rejoin the cluster.

Independent of timing guarantees consistency, clock errors and message delays in extreme cases can cause usability problems in the worst case.

Normally, a command can be completed as quickly as possible on most nodes for a round of remote calls. A small number of slow machines will not affect the overall performance of the system.

1. Next Edition

Research on the BCAC consensus algorithm is still in progress, in the next edition of the Yellow Book. We will focus on the following issues:

• RAFT+ consensus algorithm.

• Reward economic mechanism of the witnesses node.

• Side chain technology and the side chain concept of BCAC.

• The transfer of digital assets between different chains.

• BCAC's smart contract system.

1. Conclusion

BCAC committed by side chain technology and consensus algorithm to solve some issues for the block chain applications, like performance, block chain fragment, transaction fee.

Reference

1. In Search of an Understandable Consensus Algorithm <https://raft.github.io/raft.pdf>
2. Delegated Proof-of-Stake Consensus <https://bitshares.org/technology/delegated-proof-of-stake-consensus/>
3. Know your customer <https://en.wikipedia.org/wiki/Know_your_customer>