MOAC – Mother of All Chains

June 2017

[Objective]

This project is to design a scalable and resilient Blockchain that supports stateful transactions, data access, control flow in a layered structure. It creates the framework to allow user to execute Smart Contract in an efficient way. It also provides the architecture to spawn sub blockchains using underlying infrastructure quickly and easily. It is a Blockchain platform with necessary plumbing parts available to sub blockchains, providing solution for idea test, private chain deployment, complex task processing, and Smart Contract applications, etc.

[Existing problem]

Currently there are many blockchains available, but all of them suffer one or more problems.

1. Difficult to try new idea

   New idea means a new Blockchain. It requires extensive overhead to implement a new Blockchain idea, by setting up servers, develop teams, establishing community, attracting new users, etc.

2. Difficult to upgrade

   Once Blockchain has been deployed and in production, it is very difficult to add/modify/delete features. Any of those is either soft fork or hard fork. Either fork requires tremendous effort and economic consequences.

3. Incompatible among chains

   Different chains have different schemes, such as consensus protocol, currency features, and adoption requirements. These schemes prevent the interconnection or exchange among multiple chains.

4. Split participant group

   For each Blockchain, the user base is different. Mining rigs and validators are dedicated for that chain only. No two blockchains can share any of them.

[Solution Summary]

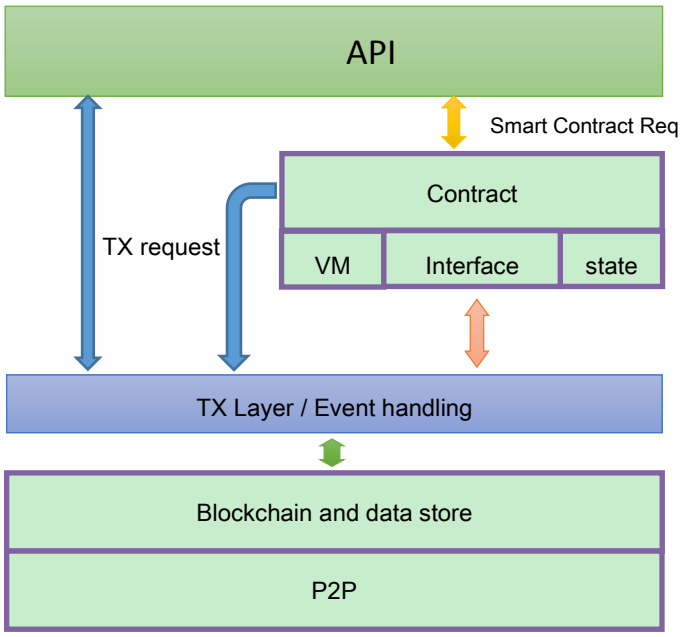
MOAC is the solution to all the problems listed above. It is the Blockchain for blockchains. MOAC itself will be deployed in public network with large number of validators. It provides following:

1. Layered configuration structure
2. Transaction, Smart Contract and Data Access support
3. Data flow, control flow and processing units, to form a distributed Von Newman architecture.

4. Validators could be configured to support multiple overlapping sub blockchains.
5. Pluggable validating scheme to support injection of user defined protocols, make it easy to deploy new sub blockchains using existing validators.
6. Encourage user with smaller processing power to participate in the validation process.

[Architecture]

Layered structure



1. P2P network layer. This layer defines p2p protocol, we will adopt GOSSIP.
2. Blockchain layer. This layer handle all operation related to Blockchain operation, like consensus, data access, etc.
3. TX layer. This layer handles TX request and reply. It also processes of the control TX request and if necessary, invokes Smart Contract related operations.
4. Smart Contract layer. This layer performs smart contract execution inside virtual machine and also keeps a temporary contract state.
5. API handles end-user input and gets the output from lower layers.

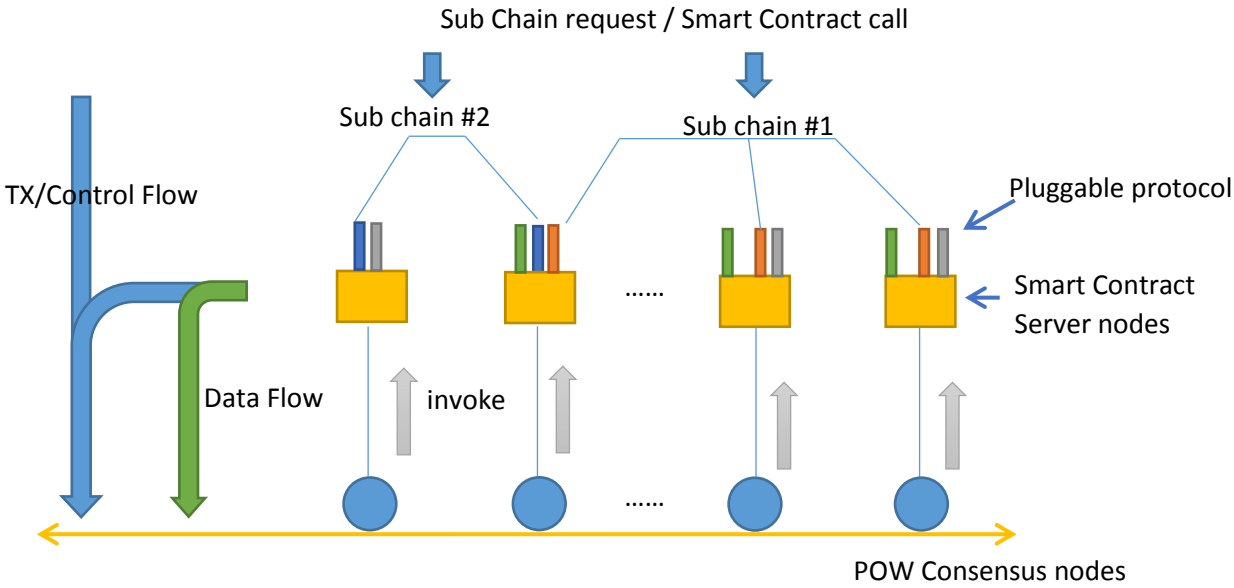
MOAC topology

Currently MOAC use POW similar to Ethereum, and adopt sharding technique to provide the underlying consensus support, with a few updates:

1. Data store is separated from transaction.
2. Consensus is agreed upon Transaction Set and Data store set.
3. Smart Contract is invoked by Transaction Set, but Smart Contract state is not directly link to transaction.
4. Smart Contract is called in an asynchronous way.

Three basic transaction types in the system: payment transaction TX_p, Data Store TX_s, Control flow TX_c. They are processed in underlying POW consensus nodes. All nodes agree on the same world state.

Besides the POW consensus on transaction and data store set, each POW node is associated with one Smart Contract Server.



The Smart Contract Server (SCS) identity is fully verifiable by the corresponding POW node. Smart contract request (create/invoke/flush) is enclosed in the Control flow TX_c and is first processed in underlying layer. Then each POW node sends the contract request to its SCS via an asynchronous call. SCS will send additional Control flow TX_c and Data Store TX_s to underlying layer if needed.

Execution of smart contract is in an efficient sharded way. All the SCS can be configured at run time to process different sections of smart contracts. The whole system throughput could be 10x-100x faster than that of traditional way. The sharded execution group marshals the sharding state into underlying Blockchain through Control flow TX_c and Data Store TX_s.

[Sub Blockchain]

MOAC system can perform regular payment transactions, data store transactions and Smart Contract transactions. Moreover, it is very convenient to utilize the provided architecture to spawn sub blockchains.

User can configure sub chain using Smart Contract to define sub chain properties (% of participant nodes, consensus protocol, policy, state storage, etc). The creation of sub chain is done through Control flow TX_c. Once sub chain is established, each participant SCS will adopt the pluggable protocol in its execution. Any following requests on the sub chain will be validated by the selected % of SCS.

The block generation of the sub chain is configured to either on-demand or on set time schedule. The on-demand feature is preferred, as it only generate blocks when needed, thus saving valuable resources.

The sub chain deployment can be as easy as sending couples of Smart Contract calls. However, it inherits the secure and robust underlying Blockchain properties. And it can reuse the large pool of existing validators and benefit from the decentralized setup.

Upgrade sub chain is also easy by just redeploying to a new set of SCS with updated chain property.

[Economic analysis]

There are two types of payments that nodes can get from contributing their computational power. Firstly, the POW nodes will get rewarded for each block they mine. This is similar to what currently BITCOIN does. Secondly, the SCS server can be rewarded for their participation of sub chains and their processing work of Smart contracts. Note that this kind of service may not be power-intensive. For example, if a sub chain is based on POS, the SCS can just spend very limited resource for the validation.

This is a big incentive to regular PC users or even mobile users. For the pure POW network, there is almost no chance for regular user to benefit from mining. However, in MOAC setup, user can setup a light POW node with almost no chance to win in mining contest, but, he can setup an SCS associated with that POW node, and gets rewarded for the SCS works it provides. This will encourage more users to join the consensus system and provide more SCS processing power. On the other hand, the Smart Cotnract owner or sub chain creator will need to pay the fee for all SCS working, but is very cost-effective considering the benefit and low startup costs. The whole process will promote a more distributed ecosystem and benefit all parties.

[Payment schedule]

Block is mined every 10s, with reward of 1 MOAC coin per block. The reward schedule halves every 3,000,000 blocks, equivalent to approx. 1 year. After block 18,000,000, the reward will be

constant of 0.04 MOAC per block. See below. We define 1 MOAC = 1,000,000 Sand. 1 Sand = 1,000 Xiao.

Block#	Reward (1 MOAC = 1,000,000 Sand)
1-3,000,000	2 MOAC
3,000,001-6,000,000	1 MOAC
6,000,001-12,000,000	0.5 MOAC
12,000,001-15,000,000	0.25 MOAC
15,000,001-18,000,000	0.125 MOAC
18,000,001-	0.1 MOAC

Transaction fee is paid in two ways. One is through Transaction. The other is for Smart Contract or sub chain.

Transaction Type	Fee	Pay to
Payment TX_p	20 Sand	POW miner
Data Store TX_s	20 Sand	POW miner
Control flow TX_c	50 Sand	POW miner
Smart Contract Call	1 Xiao	To each SCS

Smart Contract Call cost is set lower than underlying transaction in purpose, thus encouraging the usage of SCS. This can alleviate the pressure on the underlying layer, and also benefit the SCS providers.

[ICO plan]

Total pre-mined coins amount is 250,000,000. The allocation is below:

Up to 50% for ICO at rate of BTC:MOAC = 1:10,000 , with discount for first three batches

1-500 BTC: rate is 1:13,000

501-1000 BTC: rate is 1:12,000

1001-1500 BTC: rate is 1: 11,000

1501- BTC: rate is 1:10,000

30% for development team

10% for operation

The rest for reserve

This ICO targets at least 500 BTC from these crowdfunding. If we do not get the minimum target (500 BTC), all donation will be REFUNDED.

All BTC will be divided among the funders and backup team. The purposes of the ICO are to support open source project development for MOAC, marketing and Ads, exchanger, operation, or anything that we think possible to increase the value of MOAC or the usage of MOAC. All MOAC coins can be claimed once the wallet/miner release by 1 December 2017.

[Reference]

MOAC coin total amount increases over years:

ICO	250,000,000
1st year	256,000,000 (approximate)
2nd year	259,000,000 (approximate)
3rd year	260,500,000 (approximate)
4th year	261,250,000 (approximate)
5th year	261,625,000 (approximate)
6th year and beyond	261,625,000 + 300,000 * n