allonchain: A Fully Decentralized Payment System

Dali Yu

June 30, 2018

allonchain@gmail.com

Abstract. allonchain is the first blockchain records both the consensus protocol and transaction data on chain. Blocks are organized into a linear sequence over time with same structure but tagged as different types. The protocol type block only payloads consensus protocols and the transaction type block only payloads all kinds of transactions. Proof-of-Stake (PoS) algorithm is used to validate the protocol type block, and Proof-of-Work (PoW) algorithm is used to validate the transaction type block. Signatures from more than 62% of aoc token owners are required for the normal protocol type block validation, and signatures from all aoc token owners are required while the protocol type block contains constitution consensus protocol, which defines the crucial important features of the chain, e.g. the total amount of aoc, the algorithms for proof of blocks. In the PoW process for validating a transaction block, the given target hashing difficulty is related to the information of its previous mined blocks and it self's block size in bytes. As for the confirmation of the newly mined blocks, validators first load the protocol called in the block, and then use the protocol to explain and execute the payloads data. All relevant information of the blockchain, including both the consensus protocol and transaction data, are recorded and secured by decentralized peer to peer network, this is how allonchain is called fully decentralized payment system (FDPS).

Keywords: *allonchain; aoc; FDPS; PoW; PoS; blockchain; payment*

1. Introduction

Bitcoin is the world's first decentralized cryptocurrency, a form of electronic cash [1]. The probability of mining a block in the PoW algorithm used by Bitcoin and other cryptocurrencies, is dependent on how much work is done by the miner. The PoS algorithm used to validate blocks varies in that a person can mine depending on how many chain tokens they have. People not favorable of PoW algorithm hold the opinions that, PoW is prone to centralization, energy wasting and PoW systems are often very slow. For this reason, Delegated Proof-of-Stake (DPoS), a method invented by Dan Larimer, is applied in EOS [2] aims at validating transactions and form consensus by voted representatives.

Medias in the mainstream of the blockchain field had a lot of articles wrote on the comparisons between PoW and PoS / DPoS. Some of the very delusive sayings are "A tragedy of the commons for Bitcoin means that as payouts becomes smaller and smaller for Bitcoin miners, there is less incentive to avoid a 51% attack. The POS systems makes any 51% attack more expensive. Someone trying to double-spend and destroy faith in the network would have to own a majority of the coins, and the attacker would suffer from his actions [3]", and "Just like in POW, it would be unreasonable for a user to commit a fraud attack on a proof-of-stake system, unless they would be able to steal more money than they would lose by forfeiting the sum of their deposits (which is unlikely) [4]".

Just use examples to debate on those illogic views. The biggest bitcoin Asics manufacturer and the biggest bitcoin miner – Bitmain has currently gained nearly 42% of the network hashrate, would Bitmain commits a fraud attack on the bitcoin network? There is no incentive drives them to do so, on the contrary, this kind of attack even from others would bring them huge loss in mining and miner selling, possibly also suffer from bitcoins they hold. The only concern of centralization of the hashrate comes from the threat that the core developers could lose control of bitcoin. This's how BCH produced, and this issue is serious but nothing to do with the data security, Bitmain either doesn't has the incentive nor has the ability to modify the history transactions (after many confirms). What's more, the hard fork of chain is intrinsically caused by the centralization and off-chain store of consensus protocols, this could be called "fork of consensus". Therefore, blockchain should record the consensus protocols just like record the transaction data, the update of protocols should be

validated by constitution consensus, which shouldn't be changed after the chain is launched. In allonchain, we designed a 100% voting of aoc token holders for the validation of constitution consensus protocol. As for the transaction security of PoS / DPoS systems, assume there is a giant who has most chain tokens similar to Bitmain that who has the most hashing ability. The giant could sell out his tokens but still has the ability to commit a hard fork or double spent attack at any time even after a huge amount confirms. One especially serious issue for normal customers is your transactions even confirmed many times are still not safe on the PoS / DPoS based chain, since the modification of history transactions is easy and without any cost, the only thing they need to do is to make a reasonable excuse to prevent token market price drops, e.g. government requires to do so. The crucial important feature of blockchain: immutability of ledger, could not be fulfilled in the PoS / DPoS system, the currently only one feasible and well proved way is using PoW algorithm to write the transaction records on the ledger. PoS / DPoS algorithm is good for voting consensus protocols, which impacts on the future transaction operations but has no threat to the previous transaction records. This is why allonchain uses PoS algorithm to validate the protocol type block and uses PoW algorithm to validate the transaction type block.

2. Block structure

Blocks of allonchain could be divided into two types: The protocol type block and the transaction type block. The protocol type block only payloads consensus protocols and the transaction type block only payloads all kinds of transactions. Both types of block are organized into a linear sequence over time with same structure, as shown in Fig. 1. The protocol name is used to load the corresponding consensus protocol, which was recorded and verified by the previous blocks, and the height of the current block should be in the protocol's effective range. The value of the block type item could be one of the follows,

$$\text{value} = \begin{cases} 0, & \textit{protocol type block contains constitution consensus protocol} \\ 1, & \textit{protocol type block only contains normal consensus protocol} \\ 2, & \textit{transaction type block} \end{cases}$$

Each block should be hashed and treated as a number, the value must be less than a dynamically adjusted target. Hash of the block is added as a reference to the block one height higher. The timestamp keeps blocks chained as a linear sequence over time. Item

"ownerships" is a list of ownership, which is used to collect the signatures from token holders to prove the validity of protocol type block. The first ownership address is considered as the owner of this block. Fees for transaction block would be distributed to the block owner's address. Item "payloads" is a list of consensus protocol in the protocol type block and in the transaction type block, "payloads" is a list of variety kinds of transactions, including transfer of token, UTXO (Unspent Transaction Output) integration of token, deposit/withdraw of fiat-based token, and trading transaction. Nonce is an integer used to control the hashing difficulty. An important scalability feature of allonchain is that the ownerships item and payloads item are stored in a multi-level data structure - Merkle tree. The hash of a block is actually only the hash of the block header.

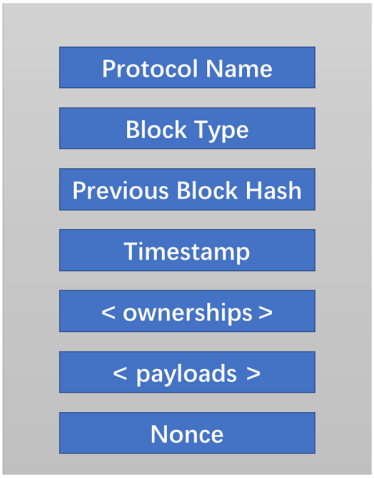

Fig. 1 block structure diagram.

3. Ownership structure

Similar to the block structure, ownership also first loads the consensus protocol and then use the corresponding protocol to explain the data. In the protocol type block, ownerships item is a list of ownership from different aoc holders. For each aoc holder U_i , has a pair of verification and signing key (vk_i, sk_i), sk_i is used to sign the message $M_{r,p}$, which is the Merkle root of the payloads. Finally, the obtained signature σ_i, the verification key vk_i and the message $M_{r,p}$ would be organized into an ownership structure data. In the validation of a block, each ownership should be self-verified,

$$Verify(\mathrm{vk}_i, M_{r,p}, \sigma_i) == True \implies Valid$$

Furthermore, PoS is required while the block is a protocol type block. If the block contains constitution consensus protocol, the total amount of aoc should be equal to the maximum

amount of aoc on the chain, that's means the 100% aoc address should sign together to prove the constitution protocols, which would happen in the genesis block, unlikely being modified after the main chain launched. If the block contains only normal consensus protocol, then holders with more than 62% aoc need to sign together to prove.

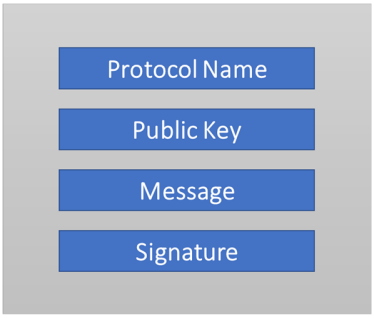

Fig. 2 ownership structure diagram.

If the block is a transaction type block, the first ownership is used to claim which address wins all the transaction fees.

4. Payload structure

Theoretically, allonchain supports to payload any types of transactions that inherited from a common structure with a self-verification interface and a size-deduction interface, which aims at decreasing transaction fees for some specific operations on chain.

Currently, three different transactions are developed,

a) token transfer, includes payment and integration
b) fiat-based token deposit and withdraw
c) token exchange

Fig. 3 shows the structure of a typical token transfer transaction. All the inputs are the previous transactions' output, and the transfer could be multi-sender to multi-receiver, the total amount of input tokens should be greater than the total amount of output token. The difference is the fee which is incentive to make this transaction being packed in a future block by the miner. If all the senders and receivers are the same and there is only one receiver, this kind of token transfer transaction is considered as integration operation, this operation could have a size deduction, which makes the integration of your UTXOs costs little fees. In this integration operation, the transaction only need to include one signature. The other kind of valid token transfer transaction is called payment, which the token transferred between different accounts.

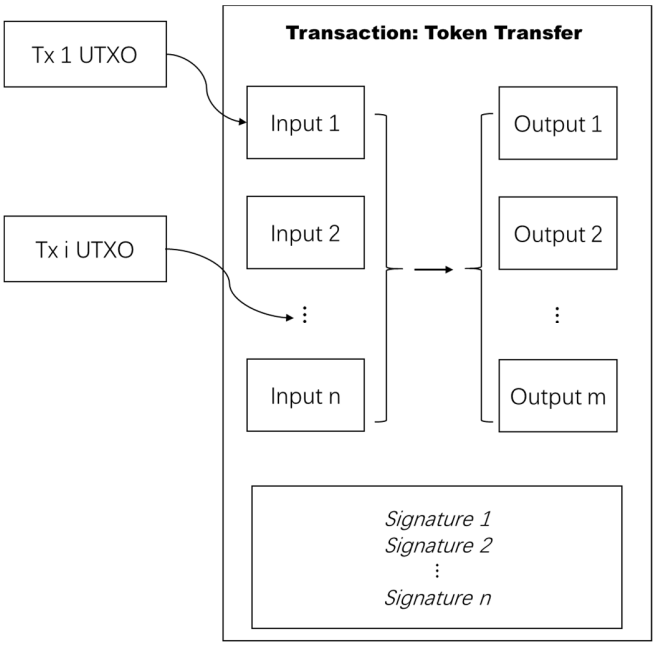

Fig. 3 token transfer diagram.

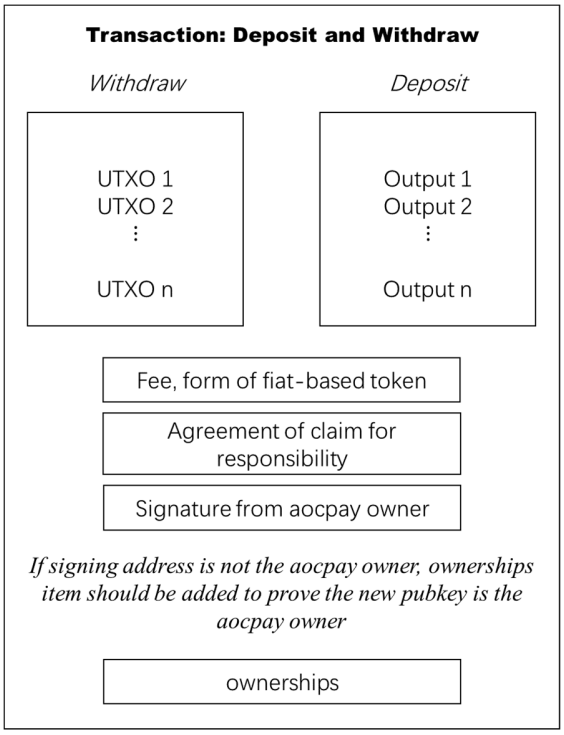

Fig. 4 fiat-based token deposit and withdraw diagram.

Fig. 4 shows the structure of a typical fiat-based token deposit and withdraw transaction. All the execution of the deposit and withdraw should be signed by the aocpay owner. The aocpay owner is

voted by more than 62% aoc tokens. Aocpay should be responsible for these operations that could bring some law issues with the real world. All the input UTXOs should be under the aocpay address, and if the signing pubkey is changed, ownerships with more than 62% aoc voting should be added in the transaction. This kind of transaction is designed for tokenize the fiat currency, e.g. Euro, US dollar, and Chinese yuan, so on. Aocpay Inc. is responsible for this service.

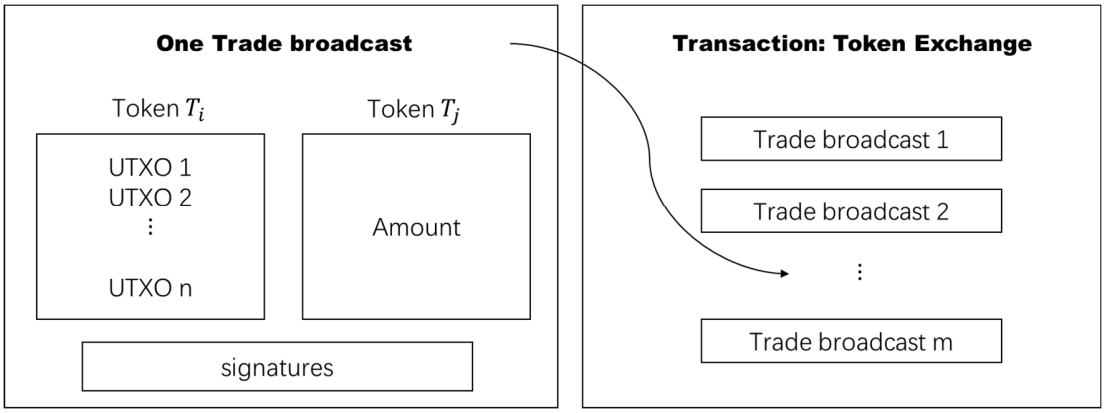

Fig. 5 token exchange diagram.

Fig. 5 shows the structure of a typical token trading broadcast and how miners organize them into one token exchange transaction. A valid transaction should keep all involved kinds of tokens have a greater amount of input than the amount of output, the difference are the fees for the miner. That means for one exchange transaction, the miner could earn fees in the form of all kinds of token involved.

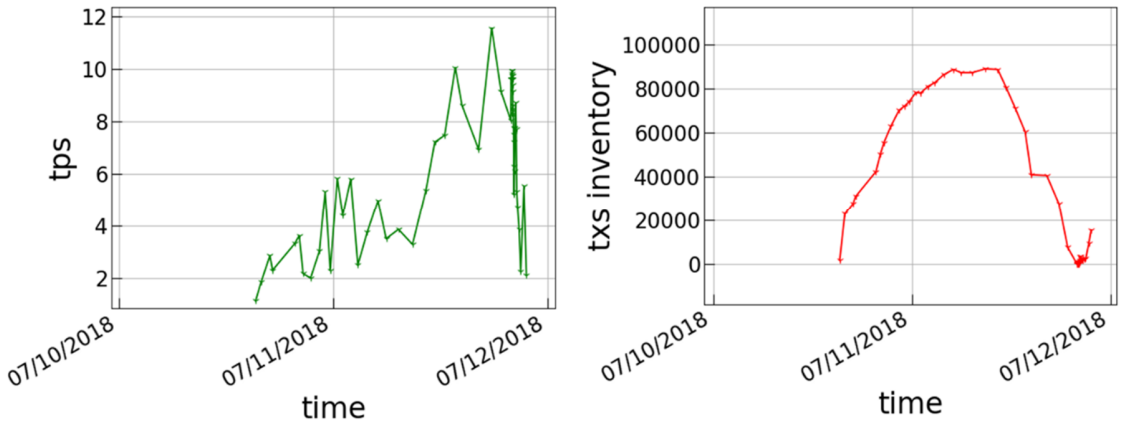

Fig. 6 a test on the transaction ability.

5. Case study

Three nodes are connected with each other in the allonchain network. Node A is a transfer node with public IP address. Node B is a mining node, packing transactions and broadcast the newly mined block. Node C is a user node, generates 5 transactions per second (tps) on average. The network starts from an arbitrary initial state. Fig. 6 shows the transaction ability of allonchain tps and the pending transaction inventory. For the Node B, the mining strategy is simple and not so smart enough to gain the maximum profit. The test result shows allonchain could achieve peak tps to be more than 10, and the network is quite inclusive to handle a sudden increase of transactions.

6. Conclusions

A fully decentralized blockchain system, allonchain, is firstly proposed to record both the consensus protocol and transaction data on chain. PoS algorithm is used to validate the protocol type block, and PoW algorithm is used to validate the transaction type block. In the PoW process for validating a transaction block, the given target hashing difficulty is dynamically related to the information of its previous mined blocks and it self's block size in bytes. Compare to traditional blockchain, advantages of allonchain can be listed as below,

1. The consensus protocol is secured peer to peer, nobody could control which protocol should be used without majority vote for the protocol. Neither hard fork nor soft fork is possible for allonchain.
2. The dynamic block design allows allonchain network to handle theoretically any amount of transactions. The network is quite inclusive to extreme conditions.
3. allonchain is fully open to implement any protocol, and smart contracts for issuing a non-fiat-based token. As planned, allonchain would implement consensus protocol for smart contract for smart contracts, which would lead smart contract into a real 2.0 era.

Reference

[1] Nakamoto Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Ian Grigg. EOS - An Introduction. 2017.

[3] https://www.ccn.com/bitcoins-future-proof-of-stake-vs-proof-of-work/

[4] https://steemit.com/eos/@eosgo/understanding-eos-and-delegated-proof-of-stake