Bytom
An Interoperation Protocol for Diversified Byte Assets

Abstract:

Bytom Blockchain Protocol (hereinafter referred as Bytom) is an interactive protocol of multiple byteassets. Heterogeneous byte-assets (indigenous digital currency, digital assets) that operate in different forms on the Bytom Blockchain and atomic assets (warrants, securities, dividends, bonds, intelligence information, forecasting information and other information that exist in the physical world) can be registered, exchanged, gambled and engaged in other more complicated and contract-based interoperations via Bytom. The protocol connects the atomic world and the byteworld to promote the interaction and circulation of assets between the two worlds. Bytom adopts three-layer architecture: application layer, contract layer and data transmission layer. The application layer is friendly to mobile and other terminals and convenient for developers to develop asset management applications. The contract layer use genesis contract and control contracts for asset issuance and management, supporting scalable BUTXO of UTXO model at the bottom layer, optimizing EVM and using introspection mechanism to prevent deadlock in Turing complete. The data transmission layer adopts DLT technology to achieve asset issuance, spending, transfer and other operations. The consensus mechanism uses POW algorithm that are friendly to AI ASIC chips. Matrix and convolution calculation is introduced into the hashing process so that the miners can be used for AI hardware acceleration services, generating additional social benefits.

1 Mission, Goal and Innovation of Bytom

1.1 Overview of the problem

In general, the information revolution has greatly changed the world we are living in. The dominance of the atomic-structured world is being challenged. In the context of the upcoming singularity of big data and large-scale computing, the Internet is transiting from "Information as power" to the stage of "computing as power". The migration of the world's economic structure and power is composed by more byte information. The information flow and byte flow that contains "negative entropy" has become a life-dependant element for individuals, businesses and institutions alike. The evolution started from:

"Byte Tool" era: Byte is used as an auxiliary product to improve efficiency. Examples are: Excel, email. Then the next stage is: **"ByteCurrency" era:** The value of symbols that exist in byte form without physical existence and media like: Bitcoin, ETH and tokens of other public blockchains and consortium chains. The next stage is:**"ByteAssets" era** that is more extensive and diverse: everything that is valuable, exchangeable in the real world will be migrated to the byte world. The rights of earning, equities, creditor's rights and securitized assets in the real world will migrate to blockchain as immutable, traceable distributed ledgers with symmetric information, which in turn interact with financial, gaming, insurance and other markets through programmable smart contracts.

There are already venues for people to buy software (byte tool) or digital currency (byte currency) like Appstore for software or Coinbase for digital currency. However, there isn't a complete and effective protocol for the transaction and interaction of diversified byte assets. Unlike the general-purpose smart contract platform like Ethereum or Quantum, Bytom is designed to be the public blockchain platform specifically for byte assets in an attempt to solve the following problems:

- *How to achieve the non-replicability of atomic assets in the form of byte assets via blockchain technology?*
- *How to establish the mapping relation between atomic assets and byte assets, and resolve compliance issue?*
- *How to bridge the gap between atomic world and the byte world to promote effective flow of assets onchain and offchain?*

1.2 Mission Statement

"Our mission is to bridge the atomic world and the byte world, to build a decentralized network where various byte assets and atomic assets could be registered and exchanged" .

Bytom will greatly promote the exchange, interaction and flow of byte information and byte assets with value attributes. New byte assets will be created by contract and configuration. Bytom will also create applications on a market-based management protocol in a decentralized way and provide unique incentives for local and global participants in the digital economy. As a medium, Bytom has been fully prepared to become an economic body to profit from information and an amplifier for information asset performance. In the future, these information assets will not only be used for existing daily work and life, but also can become the provider for AI and IOT that feeds on "data food" , which will further expand its influence on the atomic world.

1.3 Core Objectives

1.3.1 Establishment of diversified byte assets and standards

Bytom aims to build a global open platform for registration of byte assets and to facilitate the definition, creation of byte assets, and to makes it easier for users to understand.

1.3.2 Interactive tool for building diversified byte assets

Aside from being the most basic tool for asset exchange (change of ownership and swap of various digital assets following certain protocol), Bytom will also support more complicated forms of interaction, for example:

(A)Triggering tool: the asset generates a deterministic Y / N Boolean result or numerical result from a protocol-compliant vote to activate participants in the atomic world to share dataset.

(B)Forecasting tool: For example, through zero-sum game, bilateral or multi-lateral betting forecasts are generated like flight delay or winning candidate. Such forecasts could be used for hedging in financial sectors and insurance purpose in the real world.

1.4 Major Innovations

(1) Compatible with the UTXO design of Bitcoin

Bytom consists of three layers: data transaction and transmission layer, contract layer and asset interaction layer. The asset interaction layer operates on the assets by calling contracts. The data transaction and transmission layer is compatible with the UTXO model and the transaction data structure of Bitcoin to achieve high-speed concurrence and controllable anonymity.

(2) General address format

BIP32, BIP43 and ***BIP44***[1] are used in the design of Bytom wallet to provide support for multi-currency, multi-account, multi-address and multi-key with Hierarchical Deterministic Wallets (or "HD Wallets"). BIP44 provides a five-layer path recommendation: (1) to determine the path rules; (2) types of currency; (3) account; (4) change; (5) index of address. Users can control wallet for all assets by saving one master private key. BIP44 provides a good support for the change mechanism. As long as the user does not use the same address for multiple deposit, the private key is safe from exposure by saving signing transaction repeatedly.

(3) Compatible with National Encryption Standard

The asset management and operation of Bytom involves private key, public key and address system, which is achieved through ESCDA encryption and SHA256 hashing in Bitcoin' s design. Bytom will support the ***Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves***[2] and ***SM3 Cryptographic Hash Algorithm***[3] that are compliant with Chinese National standard. In terms of similar computational complexity, SM2 is much faster than RSA and DSA in processing private keys, thus a higher efficiency in encryption. The compression function of SM3 algorithm has similar structure to that of SHA-256. But the design of SM3 algorithm is more complicated. For example, two message words are used for each round of compression function.

(4) Asset naming using ODIN

The naming of assets will follow ODIN (Open Data Index Name) standards to ensure the uniqueness of assets across the entire network and blockchain. Unlike other blockchain-based identification solutions, ODIN is based on the Bitcoin blockchain and supports the introduction of other blockchains (public blockchain, consortium blockchain, private blockchain) through multi-level marking. ODIN uses blockchain height as naming index instead of registration of character string.

(5) POW algorithm that is friendly to AI ASIC-chips

By adopting POW algorithm that is friendly to AI ASIC-chips, miners could be used for AI acceleration services after they are outdated.

Bitcoin miners could be compared to AI depth as both rely on the underlying large-scale parallel computing. The vast majority of the depth learning algorithms can be mapped into the underlying linear algebraic operations. Linear algebraic operation has two characteristics: first the Tensor's flow is very regular and expectable; second is the high density of calculation. These two features make AI depth learning particularly suitable for hardware ***acceleration***[4].

Bitcoin miners have gone through four stages of CPU, GPU, FPGA and ASIC (Figure 1). In the age of CPU and GPU, the mining entry barrier is low as PC or laptop with an independent graphics card can be used for mining. With the emergence of FPGA and ASIC, the Moore's Law have its way in the world of Bitcoin mining. At present, the mining chips are measured at GH / S and the manufacturing process of wafer has been raised from 130nm to 14nm, which is close to the current limit of semiconductor manufacturing technology. However, the POW mechanism is criticized as the machines could be applied to mining only, resulting in a great waste of hardware and energy.

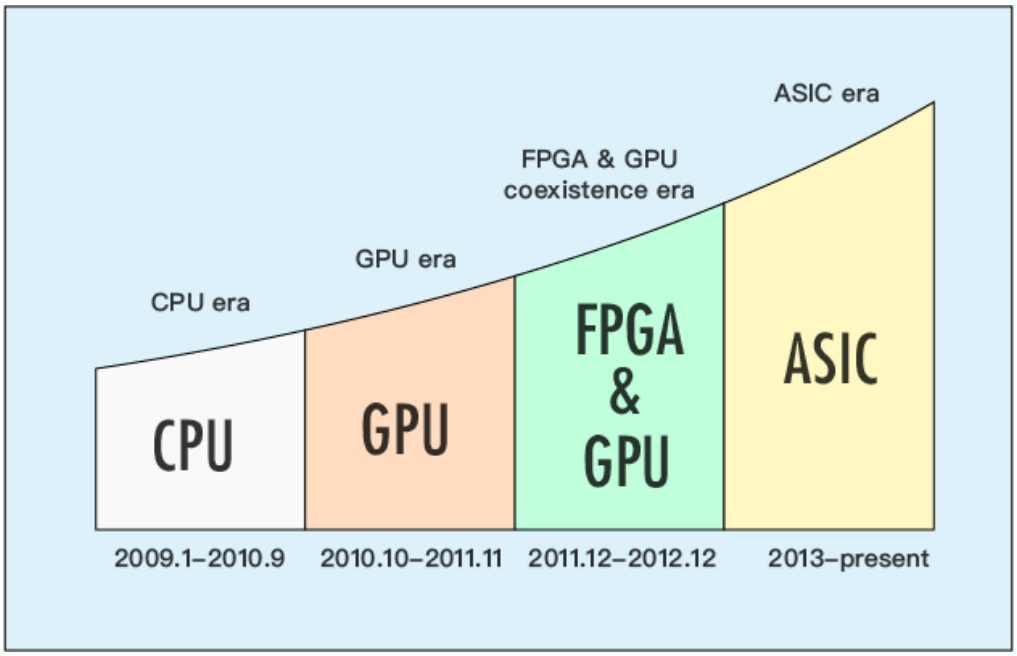

Figure 1

If we introduce matrix operations and convolution operations in the hashing process of mining, making miners friendlier to AI ASICs than GPU and CPU, then the calculation required for blockchain consensus can also be applied to the AI hardware acceleration service, which will generate greater social benefits. On the one hand, the mining market will stimulate the market for artificial intelligence, expanding needs for the depth learning ASIC chips, just like the boosting effect to GPU market lifted by current GPU-friendly PoW blockchain. On the other hand, outdated miners can be utilized for AI hardware acceleration services, saving mining costs and thus realize a win-win situation.

(6) Cross-chain asset transactions and dividends distribution through side-chain

In order to operate assets on other blockchains, developers can create a tiny version of the X chain (other blockchains) or Xrelay. Dapp developers could perform API calls via smart contract to verify network activities on X blockchain, thus achieving cross-chain communication, asset transaction and dividend distribution in the contract.

(7) Quasi "Segregated Witness" Design

In Bytom' s design, there is a DLT protocol that allows interaction between varieties of assets. Multiple blockchains that adopt the same protocol can exist independently and can be traded cross-chain, making different operators to interact in the same format. Following the principle of minimum authority, Bytom separate data and witness from signature in the design to achieve isolation between asset management and synchronized distributed ledgers. Such design achieves better programmability and contract support, and reserve interface for bypass channel in the future.

The blockchain protocol allows any network participants to define and issue assets by coding a customized "issuer". Once issued, the unit of asset is controlled by the "controller program". The controller program is implemented in Turing complete language, which can be used to write complex smart contracts.

(8) Enhanced Trading Flexibility

Unlike the Ethereum account model, BUTXO can verify transactions in parallel by adopting a mechanism similar to nonce to ensure that each unspent outputs could only be associatedwith one single transaction. In addition, Bytom is lighter than Ethereum in nature as participants only need to remember unspent outputs as the trade itself carries other relevant information (such as asset ID, units, controller program). Another feature of Bytom is: compact verification, which allows the client to verify the relevant transaction onlyinstead of all transactions in the block by trusting the amounts signed by the sender. The whole process is realized via Merkle proof. Clients can also delegate the task of monitoring the entire blockchain to their trusted servers. Blocks are upward and downward compatible via softfork. Bytom does not only support the inter-blockchain communication for blockchains that adopts the same protocol, but also need to ensure the unique asset ID. Each sidechain is forked from a certain block height of another chain, which can ensure the uniqueness of asset ID. As BVM provides enough instructions, interaction between blockchains that adopt different protocols is possible.

2 Platform Model: Three-layer Structure

Bytom will adopt three-layer structure (Figure 2):

i. Application layer: support the development of programmable Dapp, calling contracts for asset registration, written-off, trading and dividends distribution.
ii. Contract layer: account system, contractcoding support
iii. Ledger layer (data layer): permissionless public blockchain layer, POW consensus

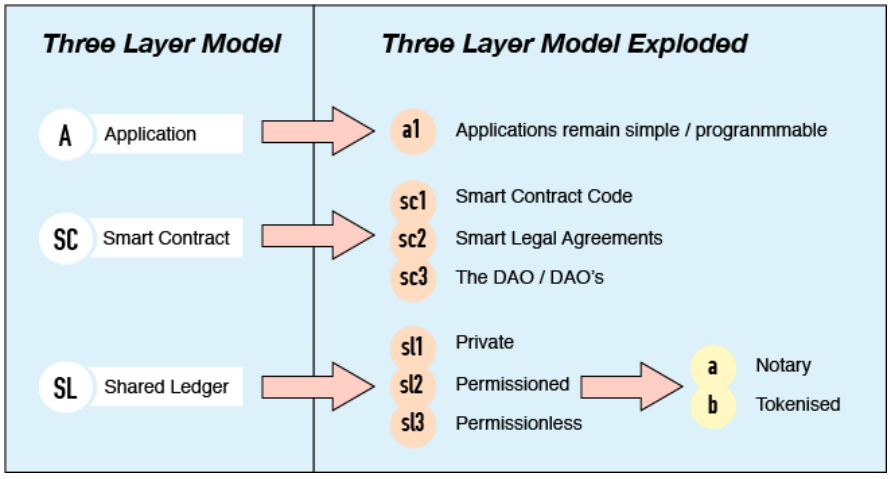

Figure 2

2.1 Application Layer:

Bytom provides various PC, WEB, mobile applications to facilitate the asset management by calling contracts. We reduce the entry barrier for application by encapsulating the underlying blockchain technology, and provide a more flexible and friendly interface for developers and asset issuers to enable them to focus on innovations of business model and business logic.

2.2 Contract layer: Contract layer design

2.2.1 Genesis Contract

The Genesis contract is a special type of contract on Bytom. The genesis contract can issue and audit smart contract and retain some access for developers, such as private key, application scope etc. The Genesis contract can execute standardization and automated audit to a certain extent to ensure that the assets released will be in line with the corresponding rules and templates. The underlying implementation of the Genesis contract will call the issuing program in the data transmission layer: Asset Issuance Program.

2.2.2 General Contract:

General contract has two functions: trading of assets and the setup and verification of dividends distribution. Such authority is open in the general control, which is equivalent to a fun in real life. If a new assets needs to be developed or introduced into the general contract, it is necessary to submit a request to the Genesis contract for approval. The underlying implementation of the General contract will call the controller program in the data transport layer: Asset Management Program.

3 Bytom’ sMaster Program and Data Structure

This function operates onData Ledger[5]layer

Bytom’ s master program contains three parts as follows:

- Asset Issuance Program is responsible for the issuance of assets
- Asset Management Program is responsible for the operations of assets like spending or exchange.

- Consensus Program is responsible for identifying which new blocks can be merged into Bytom Blockchain, which is based on POW currently.

3.1 The issuance of diversified byte assets

Bytom will support various types of digital assets. Each asset will be identified by an asset ID, which is a 256-bit string that distinguishes different asset types. By different asset ID, we can establish the asset categories and associate them withthe Asset Issuance Program and the Asset Management Program.

There are two types of assets running on Bytom network: Bytom Token (BTM) and Assets.

3.1.1 Token

Bytom token is BTM, which is a special token that is distributed to miners and nodes. The POW mechanism encourage random anonymous miners to get involved in the entire ecosystem. Distribution of the token will follow a determined supply curve.

The main uses of the BTM are:

i. Transaction fee for assets trading;

ii. Dividends of income assets;

iii. Deposits for asset issuance.

Take dividend distribution of income assets for example, if the asset issuer decides to use BTC as dividends, he can lock the corresponding amount of BTC via sidechain and convert them into BTM at market rate. This process is executed by contract calling Xrelay through cross-chain operation. For example the conversion with BTC, ETH is completed through ***BTCRelay***[6], ETHRelay (Figure 3).

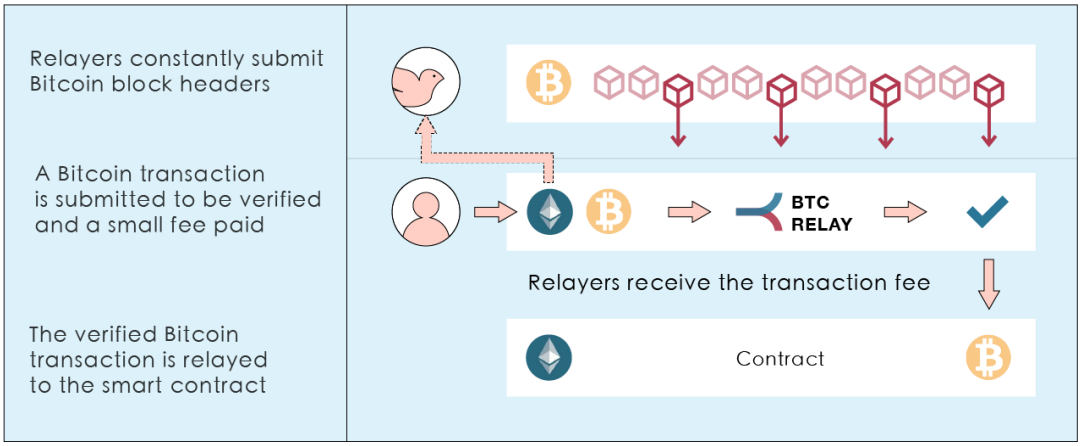

Figure 3

3.1.2 Assets

There are three types of assets on Bytom blockchain:

i. Income assets: income assets include film making, home-stay property,fixed assets invested by local government, non-performing assets etc.

ii. Equity assets: Equity assets include equity of non-listed companies, equity of private funds, shares of non-public internet investment etc. The transfer of equity assets requires qualified investor verification.

iii. Securitized Assets: Securitized assets, including debts, automobile loans and other asset-backed securities that can generate predictable cash flows and whose credit can be enhanced through structured design.

3.2 Exchange of Onchain Assets

In this section we will discuss the most basic functionality of Bytom, or the "asset exchange" section described in 1.3.2. The function will be achieved in the first version of Bytom.

Trading of asset dividends, ownership and the right to use: internal transfer between accounts under the same contract

The redemption of assets: BTM transfer via contract

Account is an abstract concept of Bytom and runs on contract layer. Each account is associated with a set of BUTXOs at the date ledger layer. The sum of all the BUTXO assets under the account is the balance of the account.

The following are the basic concepts of the Bytom data model:

Transactions

A transaction is a basic operation of Bytom Assets, which contains a data structure with values of inputs and outputs.

Inputs

Can be one or different types of digital assets, or an output of a certain transaction;

Outputs

Determine the outcome of the asset transaction, which is an asset operation program that specifies the way in which the output will be spent in the future.

The following figure (Figure 4) is transaction using USD, EUR as example, which could be replaced with BTC or ETH. The same applies to other examples.

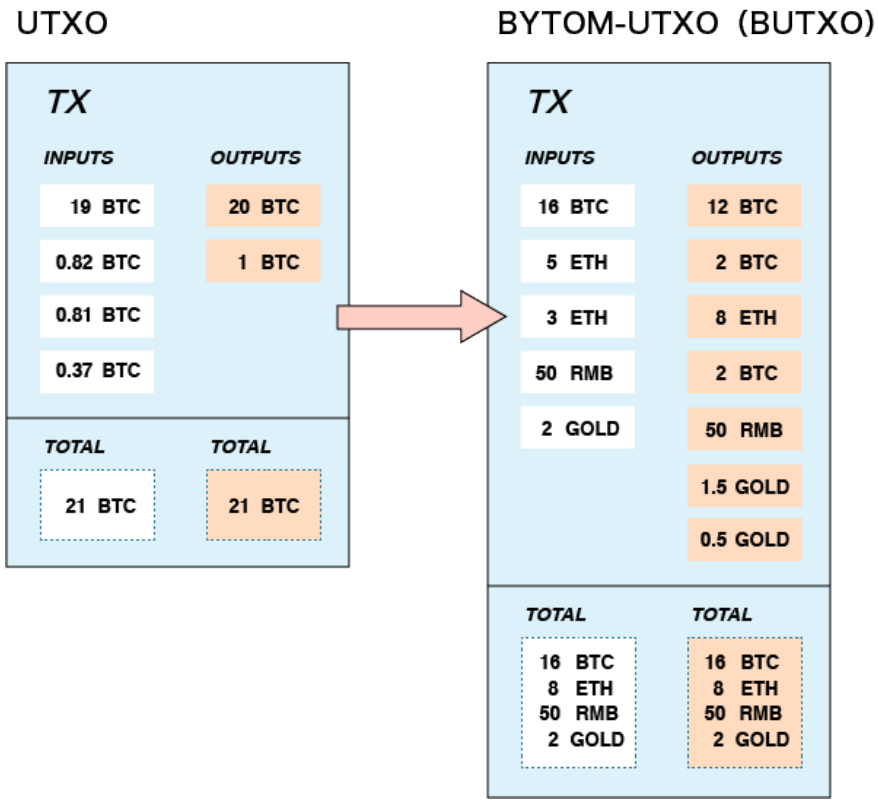

Figure 4

The inputs of each transaction must be a set of newly generated asset units, or a result of a set of BUTXO returned by an asset operation program. Both types of inputs must be verified by the above-mentioned Issuance Program.The verification process of the issuer program is to pass parameters to the Witness Field of the transaction and transaction will be executed if verification is approved (Figure 5). This part is somewhat similar to the "Segregated Witness" of BIP141.

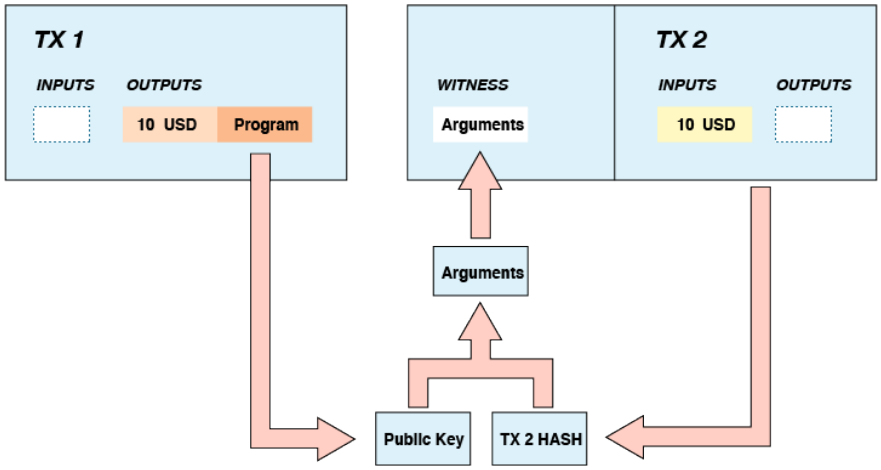

Figure 5

For example, the Asset Issuer program and the Asset Operation program can initiate a authenticity verification. A certain message is hashed and signed, then the hashing value and the signature of which could be used to verify whether the signature is signed by the private key corresponding to the public key.

BUTXO

In order to prevent double spending and to improve the transaction concurrencyand processing efficiency, Bytom introduces a basic transaction unit:BUTXO (Bytom Unspent Transaction Output), whichis scalable and supports multiple asset types (Figure 6). Once a transaction uses a particular output,the same output cannot be usedby other transactions.A general BUTXO pool is maintained by the Bytom network, inputs of all blocks will actually be associated with the existing one or more BUTXO.Once a transaction is confirmed, all spent outputs in the transaction are removed and new unspent BUTXO outputs are added in the pool.

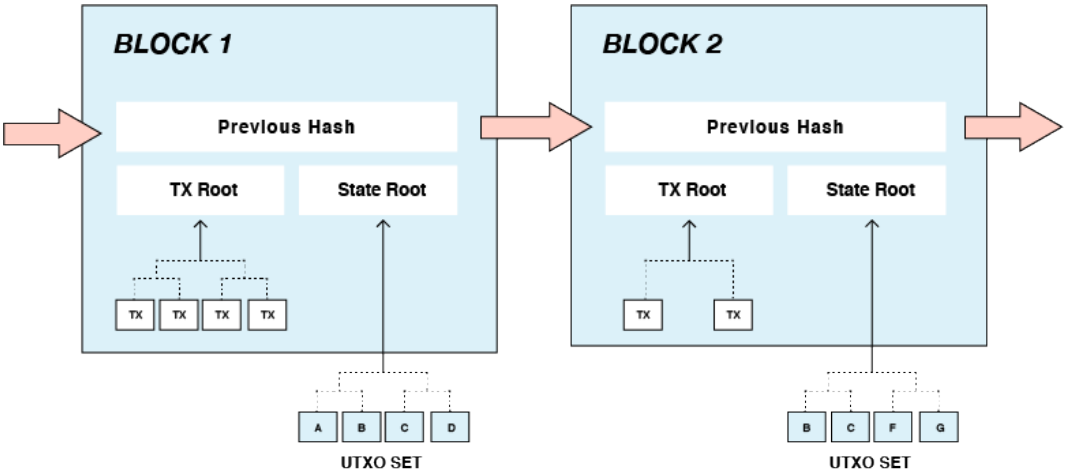

Figure 6

Block

One or more transactions of Bytom are packed into blocks. Header of each block contains hash value of previous block and connected accordingly to ensure the immutability of the blockchain. Each block contains hashing of all transactions in that block and the hashing snapshot ofexisting BUTXO. The two hashes areconnected to the roots of two Merkel trees. Simplifiedidentification and verification of transactions and BUTXO could be viathe two Merkel tree.

3.3 Consensus Mechanism

In order to ensure the security of the transaction data of the entire block chain, the block generation needs to follow a certain Consensus Program. The consensus program of a secure asset blockchain should include the following attributes:

(1) Verify the authenticity of the transaction: transaction authenticity verification only involve with the public-private key pair.A single participant can generate and use multiple key pairs.

(2) Non-repudiation: participants of a transaction cannot deny the occurrence of the transaction.

(3) Integrity: transaction cannot be modified.Transaction is broadcast the peer-to-peer network once it has been created.

In accordance with the principle of the ***minimum viable blockchain***[7], transactions needs to be packed into blocks, making the miner fee relatively low compared to the value of the asset.Valid block requires effective PoW, which is difficult to provide but

easy to prove. PoW is achieved through hashcash algorithm, which is built on top of energy cost, thereby increasing the cost of generating valid blocks, making the cost unbearable for malicious attackers.

Bytom focuses on providing a blockchain solution particularly for assets. The project requires the majority of nodes to reach a strong consensus so thatthe entire system is not vulnerable to Sybil attack and 51% attack. Therefore performance is sacrificed to meet the demands of decentralization and security (comprehensive integrity) as described in the ***Impossible Triangle***[8].Built on top of the PoW mechanism of Bitcoin and Ethereum, Bytom proposes a consensus algorithm that is friendly to AI ASIC chips so that the hashing power can be applied to the AI hardware acceleration service, thus solving the hardware consumption problem of PoW miners.

3.4 Virtual Machine (BVM)

Bytom's virtual machine is a stack-type state machine: all instructionsare executed on the stack. The instruction set of BVM is Turing complete.Run Limit is adopted to prevent the deadlock and could be set through network consensus. Pricing of Run Limit depends on the operation consumption. This is very similar to the gas mechanism of Ethereum. The difference is that BVM will not price run limit in each transaction. BVM containssome basic instruction set like push, pop and other complex mathematical encryption operations like SHA3, CHECKSIG, and CHECKMULTISIG etc.

Introspection function

Transaction introspection: can be in the implementation process to determine whether more than a predetermined time, you can also bring their own control procedures, to (price, assets, running process, index) to do some free control.

Block introspection: Introspection instruction set (BLOCKHASH, NEXTPROGRAM), can only be implemented in the consensus program.

Because of the rich set of instructions, you can combine the completion of the transaction is not just signed and signed the function. Such as multi-signature, multi-signature, early deployment (such as similar WeChat red envelope function, A to B to send the transaction, need to confirm B to the chain) CHECKPREDICATE provides a powerful other cross-chain functions, including the realization of similar to BTCRelay function.

4. Application Scenarios

4.1 Scenario A: Management of Income Assets

Bytom can be used for management of income assets. Blockchain can eliminate the information asymmetry in the fund-raising campaign, operation and follow-up funds of a crowdfunding project, reducing the trust costs. Built-in smart contract is available when issuing crowdfunding assets through the programmable interface provided by Bytom so that funds are spent as it is designed for. Smart contracts also guarantee that if a scheduled goal is not reached, funds can be automatically returned to the investor's account. All of these operations do not require third party endorsements or commissions paid to third parties.

The advantages of managing crowdfunding projects via Bytom are:

(1) Transparent rules and audits: When investors participate in Bytom-based projects, a permanent and immutable record is kept. The subsequent spending of these funds is also kept in an open and transparent ledger that anyone can access. These features offer the level of trust and security that traditional payment processors and auditors cannot provide. (2) Better liquidity: crowdfundingbackers can trade their assets quickly and simply with others via Bytom. The transaction can be done on the p2p exchange through the custody feature of Bytom.

4.2 Scenario B: Management of Non-listedCompany Equity

Non-listed companies are usually weak in handlingequities, options, funds and process due to the restriction on spending. For example, a medium-sized financial institutions need to hire professional lawyers and accountants to managecompany assets due to the complexity of company structures. Startup company, which receives investment from investment institutions, could expand their network through business investors at lower cost.

The asset management feature of Bytom targets three types of users: first, companies can reduce their cost on managing equities and options and extend their funding raising source; second, private equity fund managers can issue contract-type fund through Bytom; third, the lawyers can sign off their work after completion of legal services to enterprises via Bytom.

Bytom offers enterprise with convenient asset registration, management and exchange system, and to build an efficient and credible platform for investment and

financing. A blockchain asset registration and exchange platform usually offers the following services: design of share structure, design of shareoptions andthe management, online creation, distribution, authorization planning of option maturity, online creation, granting, approval and signoff of agreements. The platform should also provide enterprises and incubators with customized legal consultation both online and offline so that executives can monitor the status of assets in real-time understanding of equity status and management, so as to create a substantive endorsement of the asset network. Changes in corporate governance can be done through an online smart contract + electronic sign, eliminating the need for complex paperwork.

Bytom is also applicable to the contract-type fund management. Private equity fund managers use Bytom to issue the contractual fund. Asset audit, investor feedback rules, repurchase rules and transaction rules are defined in the smart contract, which will make the whole management process transparent and legally compliant. It' s easier to transfer and trade fund shares. Investors can be assured to purchase long-term equity investment fundswithout worrying emergent needs. Through the transfer system of Bytom, investors can trade their shares any time.

4.3 Scenario C: Securitized Asset Management

Asset Backed Securities (ABS) refers to the assets that lacks liquidity but have future cash income. These assets are transformed into securities that are tradable in financial market through structural reorganization.

There are 3 steps to securitize assets. First, the issuer is to set the asset to a SPV (Special Purpose Vehicle), the second step is to separate the SPV into shares and the last step is trading. The traditional process is complicated and inefficient. A company that wants to issue shares must first sign contract with a broker. The approval process is lengthy and complicated before investors can apply for investment. In addition, even when the shares are traded in the market, there are a few days between the securities trading day and the settlement day. With blockchain technology, ABS can be simplified into three steps: one is the right registration; second is the tokenization of the asset; third is the transactions of smart contract.

Management of securitized assets via Bytom can greatly improve the efficiency, safety and traceability of ABS operation. The system can also store transaction data safely, ensure that information cannot be forged and modified, and automatically execute smart contract. All the market participants in the ABS trading could be kept informed of the asset registration and transaction information simultaneously through

distributed ledger and consensus mechanism, which effectively solve the settlement issue between agencies.

Reference:

[1]**BIP44** https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki

[2]**Public Key Cryptographic Algorithm SM2 Based on 3.Elliptic Curves**
http://www.oscca.gov.cn/News/201012/News_1197.htm

[3]**SM3 Cryptographic Hash Algorithm**
http://www.oscca.gov.cn/News/201012/News_1199.htm

[4]**Wang Kui: Beyond CPU and GPU (Notes on TPU-powered Alphago)**

http://dwz.cn/67GUGv

[5]**Chain** https://chain.com/

[6]**BTCRelay** http://btcrelay.org/

[7]**Ilya Grigorik Minimum Viable Block Chain**
https://www.igvita.com/2014/05/05/minimum-viable-block-chain/

[8]**Changjia: Impossible Triangle: Security, Pro-environment and Decentralization**
http://www.8btc.com/impossible-triangle