myDexChain

+ + +

++

Whitepaper

myDexChain Technology

myDexChain is the fastest and most efficient blockchain technology. Thanks to myDexChain, you can greatly benefit the universe and yourself. myDexChain for a sustainable technology.

dexplorer.mydexchain.io

mydexchain.io

dexfactory.mydexchain.io

01. Framework
Framework & Implementation

01

The overall technical architecture consists of two platforms:

1.Blockchain Platform:
a core blockchain-based functional module is offered:
(1) Contract layer: a multilingual smart contracts platform;
(2) Consensus layer: a Fast PoS-based PoS consensus algorithm.

P2P-based distributed storage system:
a support located at the bottom:
(1) Network layer: customized content-addressable P2P storage network;
(2) Data layer: data storage is based on DB

01. Framework

Blockchain Platform

Introduction

myDexChain contains consensus engine, ABCI, UDXO, smart contracts and other modules. Consensus engine is the core, application connects with consensus engine by ABCI to form a Byzantine fault-tolerant state machine, which can be implemented in any programming language.

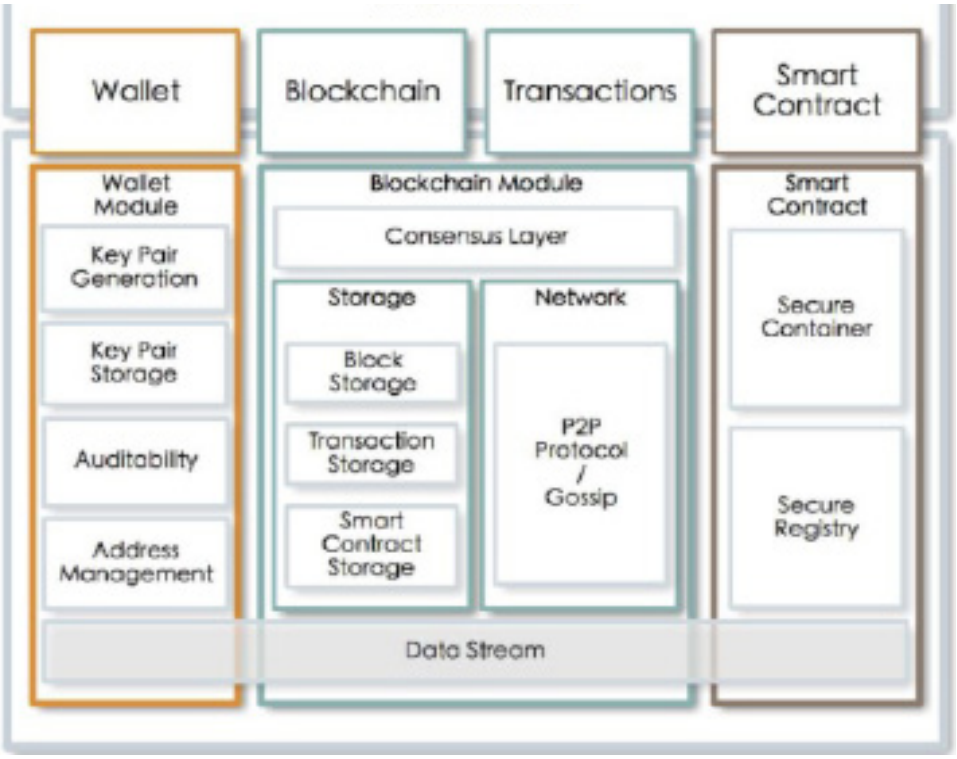
myDexChain blockchain platform has the following characteristics:

1. Scalability: myDexChain blockchain can be extended through the side chain, which means that not only currency transactions, legally binding contracts and certificates, audio and video files can be stored in the blockchain database;
2. Decentralization: Without an agency, all nodes have the same rights and obligations, any node stopping working will not affect the overall operation of the system.
3. Trustless environment: All nodes in the system can be traded without trust. Because the operation of the database and the entire system is open and transparent, the nodes can not deceive each other;
4. Consistency: The data information between nodes is consistent;
5. Fault-tolerant: The system can accommodate 1/3 node Byzantine failure;
6. Scalability Account Model: UDXO Model + Account Abstraction.

myDexChain has also made targeted improvements on the premise of UDXO‘s easy-to-parallel computing model. To make data easy to manage and easy to program, myDexChain introduces the world state-lightweight state tree concept, each of which maintains a global world state, the global state has the features of quickly find, can not be changed, easy to provide proof.

01. Framework
Blockchain Platform

Software Hierarchy



Software level is divided into two parts. The first part includesAPIs, SDKs and CLI, which are mainly used for calling an external provider for convenientdevelopment.The second part includesWallet Module, Blockchain Module and SmartContract Module, provides a storage interface, making the data of each modulepersistent.

01. Framework

Blockchain Platform

„UTXO“<UDXO

In the UDXO model, it is possible to transparently trace back the history of each transaction through the public ledger. The UDXO model has parallel processing capability to initialize transactions among multiple addresses indicating the extensibility.

Additionally, the UDXO model supports privacy protection in that users can use Change Address as the output of a UDXO. The target of myDexChain is based on smart contracts.

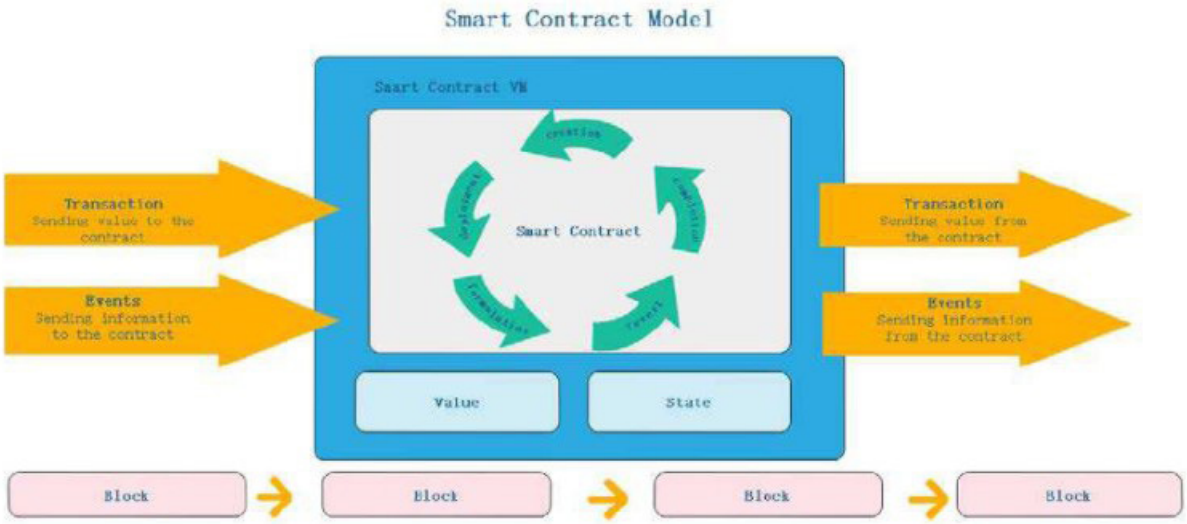
Compared with the UDXO model, Ethereum is an account based system. In Ethereum, balance management resembles a bank account in the real world. Every newly generated block potentially influences the global status of other accounts. Every account has its own balance, storage and code-space base. users perform P2P transactions via client remote procedure calls. Although sending messages to each account via smart contracts is possible, these internal transactions are only visible in the balance of each account and tracking them on the public ledger of Ethereum is a challenge.

Based on the discussion above, we consider the Ethereum account model to be a scalability bottleneck. By contrast. The UDXO model of bitcoin has enhanced network efficiency with obvious advantages. Therefore, we build the block-chain based on the „UTXO“<UDXO model and abstract the concept of the account, making it more intuitive understanding of the real world, which is the original intention of myDexChain.

01. Framework

Blockchain Platform

Smart Contract



Certainty and Termination are two properties of a smart contract. When designing a smart contract system, non-deterministic factors need to be excluded.

Bitcoin has a set of scripting engines, the instruction set is very simple and non-Turing complete, with termination, so bitcoin smart contracts are certain. The Ethereum Virtual Machine (EVM) is a runtime environment for Ethereum smart contracts. The system functions for Ethereum smart contracts are not nondeterministic, but the contract‘s call path can be nondeterministic and result in a scalable performance Losses, it uses meter to achieve the termination. The Hyperledger Fabric smart contract uses Docker as the execution environment. Docker is a lightweight virtualization technology, under the blockchain Docker is a “heavier” execution environment, which is where the performance bottlenecks of Fabric, currently only up to hundreds of TPS per second, which uses a timer to achieve Termination.

01. Framework
Blockchain Platform

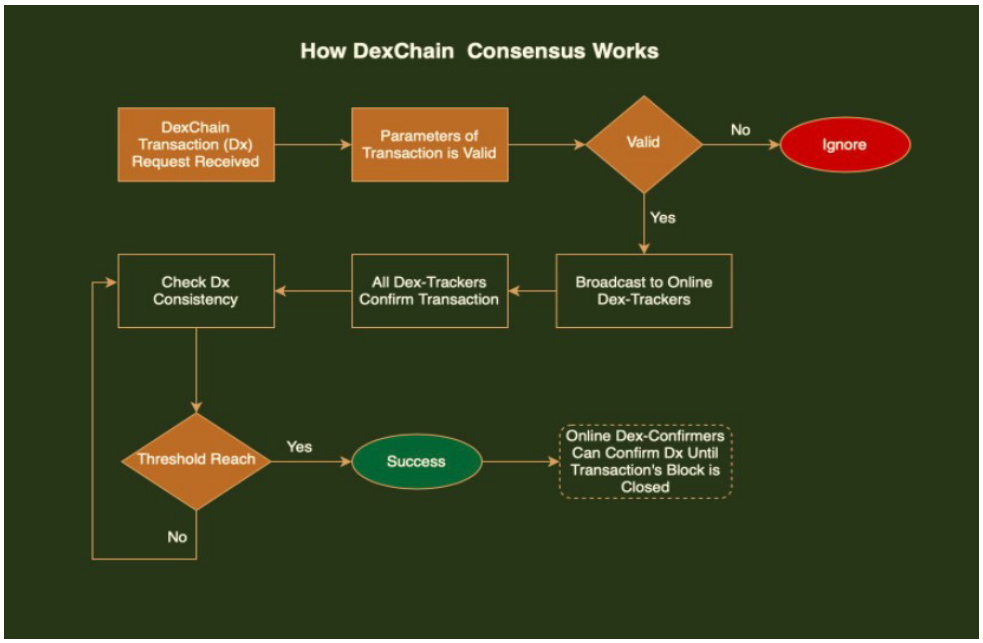
In order to keepwith the advantages of certainty, termination, and lightweight of virtual machines and the language flexibility of container programming, myDexChain is poised to develop the myDexChain Virtual Machine as an execution environment for its smart contracts in the future. The MVMboots very fast, occupies less resources. myDexChain virtual machine data manipulation instructions are directly to the array and complex data structures to provide support. These will enhance the operational performance of myDexChain smart contracts. The myDexChain Network plans to charge for the operation and storage of tokens and smart contracts to achieve economic incentives to book-keeping persons and to prevent the abuse of resources.

In the future myDexChain smart contract developers can use almost any high-level language they are good at for myDexChain smart contract development. The first language support are java, Go etc. myDexChain plans to provide compilers and plug-ins for these languages to compile high-level languages into the instruction sets supported by myDexChain virtual machines.

The myDexChain smart contract model shown above is a piece of code (a smart contract) that runs on a smart contract virtual machine and is deployed on a shared, replicated ledger (blockchain). myDexChain has a life cycle for smart contracts management, respectively are: the establishment, deployment, development, rollback, termination. It can maintain its own status, control its own asset value and receive external information, transactions or external information and transactions to respond.

01. Framework
Blockchain Platform

Consensus



The consensus of myDexChain adopts a three-step strategy. The first step is to adopt a adorno-based technology system to implement a centralized consensus algorithm. The purpose of myDexChain is to achieve system joint debugging and functional integration.

The second step is to use Raft-based distributed consensus mechanism to realize the centralized and distributed leapfrogging. This step gradually improves the functions of network and distribution and lays the foundation for the eventual realization of a wide distribution with no logical center.

myDexChain is currently open source code to achieve a consensus algorithm for the first phase of the center. The second phase of the distributed consensus algorithm is under development and testing.

01. Framework

Blockchain Platform

Protocol Buffer based object coding and serialization

Example

Proto code:

```
message Block {     repeated Transaction transactions = 1;
BlockHeaderblockHeader = 2;
}
```

Serialization:

```
Block.Builder block = Block.newBuilder()
.setTransactions(transactions)
.setBlockHeader(blochHeader)
.build();
byte[] blockData = block.toByteArray(); byte[] keyData = block.getHash();
DB.saveBlock(keyData, blockData);
```

Deserialize:

```
byte[] keyData = block.getHash();
byte[] blockData = DB.getBlock(keyData);
Block block = Block.parseFrom(blockData).toBuilder().build();
```

01. Framework
Blockchain Platform

Proof Of Stake

The proof-of-stake algorithm uses a pseudo-random elimination process, which is a combination of factors such as share age, randomness, and the amount of coins the node owns, to determine the node that will be the validator of the next block. Users who want to participate in the block creation process must lock a certain number of coins as their own shares in the network. The size of the stake determines the chance that a node will be selected as the node to approve the creation of the next block. The larger the stake, the greater the chance. Different methods are also added to the selection process so that the process does not favor the wealthiest nodes in the network. The two most commonly used methods are ‚Random Block Selection' and, Coin Age Selection'.

The main advantages of the Proof of Stake algorithm are energy efficiency and security. More users are encouraged to become nodes as it is easy and low cost. However, randomizing the process makes the network more dispersed (decentralized) as it makes mining pools unnecessary for mining blocks. Less need to create new coins to be awarded as a reward also helps keep the price of that coin more stable. In order to efficiently control the network and approve fraudulent transactions, a node must have a majority stake in the network. This is also known as the 51% attack. Depending on the value of the cryptocurrency, it is very difficult to implement as controlling the network requires owning 51% of the circulating supply.

01. Framework

Blockchain Platform

Technical characteristics and contrast

Bitcoin vs Ethereum vs myDexChain Overall Technology Comparison

COMPARING TO OTHER BLOCKCHAINS

	BITCOIN	ETHEREUM	POLKADOT	AVALANCE	myDexChain
Transactional Throughput	7 tps	14 tps	1.500 tps	> 4.500 tps	10.000 tps CPU - Bound
Transactional Finality	60 min	6 min	60 sec	< 2 sec	< 1 sec
Energy Efficient	No; ASIC-Optimal	No; GPU-Optimal	Yes; CPU-Optimal	Yes; CPU-Optimal	Yes; CPU-Optimal
Number of Validators	3 Pools w >51% hash rate	2 Pools w >51% hash rate	>200 Nodes relay chain	Thousands of node	Unlimited DexTracker (DexNode)
Sybil Protection	Proof of Work	Proof of Work	Proof of Stake	Proof of Stake	Proof of Stake
Safety Threshold	51%	51%	33%	80% parameterized	51% | Semiotic
					Build Now <->

01. Framework
Blockchain Platform

myDexChain Protocol Definitions

DRC-8: The first and main coin of myDexChain technology is DexChain. DexChain is subject to the DRC-8 protocol and Dexchain will be charged as a fee for each transfer in myDexChain technology for the subcoins to be created.

DRC-16: The subcoins to be created will be subject to the DRC-16 protocol. Each business will be able to generate its own crypto value and create its own ecosystem.

DRC-32: In the DRC-32 protocol, the safest survey and election systems can be created here.

DRC-64: Internet of things can be created in the DRC-64 protocol. For example, we can say that a cargo company follows and records each step of the process of receiving a cargo from the sender and delivering it to the recipient.

DRC-128: Protocol is defined for artificial intelligence applications.

01. Framework

Blockchain Platform

P2P network

Centerless, but secure user registration, is implemented through the blockchain mechanism, and the same mechanism has been applied in Bitcoin without the need for central authorization, which avoids double spend difficulties. The blockchain ensures no duplicate registration, and the newly-registered users must obtain the confirmation of multiple blocks before taking effect, i.e. notarization. Each block is defined as:

$$Block_i = [i, H(Block_{i-1}), Nonce_i, SpamMsg_i, [UserReg_j, UserReg_{j+1}, ...]]$$

H (Blocki) provides Proof-of-Work to prove that the user received satisfying Nonce value in Noncei space through violent solving; meanwhile occasional hash collision is avoided through verification. The difficulty of solving is determined by the difficulty value, and the number of blocks generated per hour is automatically set by the system, which is similar to the Bitcoin network.

$$UserReg_j = [Username_j, PUBK_j, Nonce_j]$$

New user j must broadcast UserRegj when registering online, and after receiving the broadcast message, other nodes must prove the proof-of-Wo rk of H (UserRegj), which will prevent denial of service attacks by false registration. This workload is much smaller than the workload of the blockchain; typically, a few minutes of computation can solve the problem.

The blockchain provides a mapping from the user name Usernamej to the user public key PUBKj, a dictionary that can be publicly queried.

01. Framework
Blockchain Platform

Dex-Tracker HDD-SSD Earning System

When we examine the context of myDexChain, which is designed as decentralized systems, DexChain‘s design is censorship-resistant and does not require intermediaries for inter-user transactions (no matter how far they are in the world), what makes it possible to use it as a peer-to-peer (P2P) decentralized digital currency is the computer NODE‘s network. Full nodes are ‘nodes that provide real support and security to myDexChain and are indispensable for the network. These nodes are also called validating nodes as they work in the process of verifying transactions and blocks in line with the consensus rules of the system. Full nodes can also transfer new transactions and blocks to myDexChain. Full nodes should be kept in physical servers or PCs connected to different IP addresses in order to be decentralized and secure. Many volunteer organizations and users serve as a myDexChain Full node holder to assist the myDexChain ecosystem. There must be node holders in every blockchain network. However, the difference of myDexChain ecosystem from others is that it gives its supporters award coins in return for this service. There are approximately 600 full node holders in the myDexChain network. (You can visit dexplorer.mydexchain.io/dextracker). MyDexChain full node holders must have a minimum of 1 DexLife in order to earn reward coins. Users who own a DexLife package are identified by myDexChain Dex-Tracker number. With this number, users who want to keep a full node can install them on their physical servers or computers and win prize coins. You can get dual gain. Don‘t forget to check out the Dex Factory section.

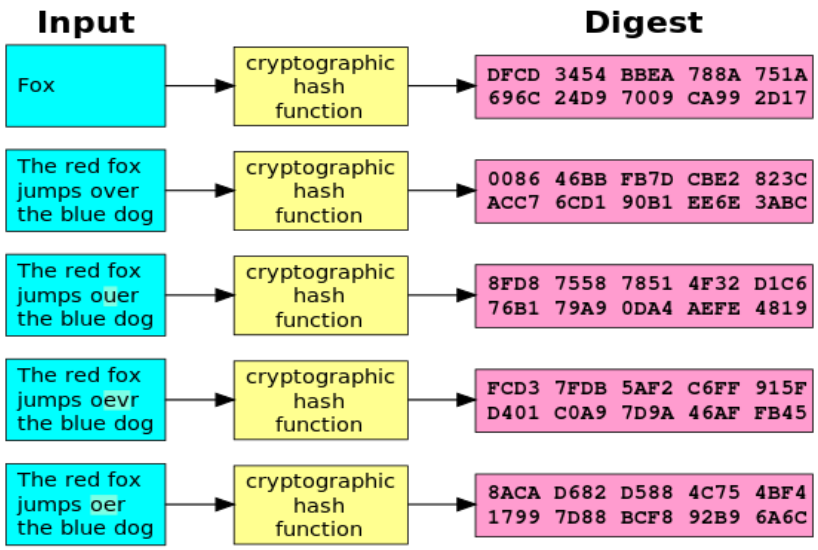
01. Framework
Blockchain Platform

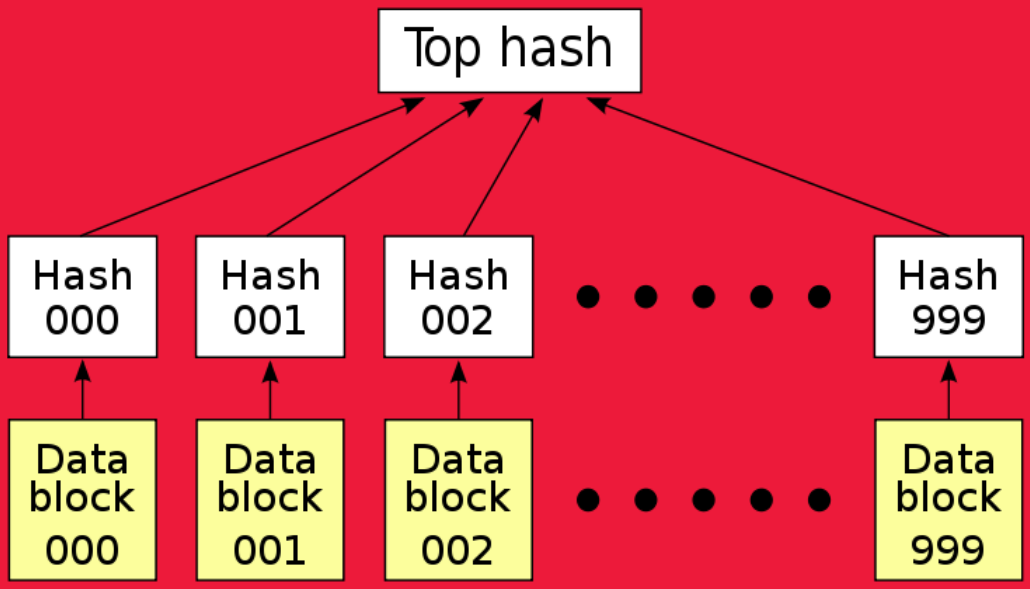
DRC-32 Survey Protocol

The biggest contribution of myDexChain technology to the blockchain ecosystem is the survey protocol. In this way, it includes security along with the hash algorithm. The benefit to ecosystem is invaluable. In this way, companies, associations and even government elections will be able to be made through the myDexChain platform.

SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA), first published in 2001. They are built using the Merkle–Damgård structure, from a one-way compression function itself built using the Davies–Meyer structure from a (classified) specialized block cipher.

The output size in bits is given by the extension to the „SHA“ name, so SHA-224 has an output size of 224 bits (28 bytes); SHA-256, 32 bytes; SHA-384, 48 bytes; and SHA-512, 64 bytes.





DRC-32
Survey Protocol

You will find the shortest way to reach your users with mydexchain. Thanks to instant feedback, you will get reliable and precise results beyond the classical survey systems and most importantly, thanks to the hash algorithm.

More Efficient Surveys Through Smart Contracts

01. Framework
Blockchain Platform

Dex-Confirmer Algorithm

Miner approval times vary according to the infrastructure of the blockchain, the algorithm it uses, and the mining method. Generally, blockchains with Proof of Work (PoW) mining take longer to confirm than for Proof of Stake mining. The fact that each cryptocurrency's miner confirmation time is different is due to the block found times. While the block finding time in the Bitcoin blockchain where the blocks are verified with Proof of Work mining is around 10 minutes, the block time in the Ethereum blockchain working with Proof of Work mining is around 15 seconds. In myDexChain, this time takes 1 second. On the myDexChain Blockchain, one Block closes every hour while the other Block remains open. The closed block is presented to the users for 1 hour. In other words, Transfers automatically get 15 confirmations and take place. They queue up to be confirmed on the open Block. When the block closes, validators begin to approve. Until the next block is closed, confirming users can make their transactions. Approved blocks take their place in the chain.

01. Framework

Blockchain Platform

DexChain Mobile Wallet

The myDexChain network is a new distrubuted DeFi technology, known as blockchain in the world, with high reflexes, specially designed on the dynamics of commercial life. With this app, you have a standolone wallet in the myDexChain network and more.

DexChain, which can be used as a payment system in any small or large commercial activity, has its own blockchain technology. All turnover from commercial activities is distrubuted to the community through smart contracts.

With this wallet, you can do anything on behalf of DexChain.

myDexChain

myDexChain is the fastest and most efficient blockchain technology. Thanks to myDexChain,

Whitepaper

mydexchain.io