

## Multichain

Multichain is a free and open source blockchain platform to create private/per- missioned blockchain networks. Multichain is an extended version of the bitcoin core software. The bitcoin engine provides security peer communications to Multichain.

### Language support

The thing which makes Multichain more powerful is its support to 5 high-level languages, they are Python, JavaScript, and Ruby, Php, and C#. Multichain provides a simple API and a command line interface for the application development. The developer can download Multichain packages for all those languages from Github repository and start development. Multichain doesn't use cryptocurrencies and smart contracts. So that financial transactions are not possible with it.

Compared to other blockchain platforms average block time is very low in Multichain and it is about 2 seconds. But the speed increases the chance of hash collisions.

### Security

The main feature of a Multichain is that the visibility of blockchain activities are kept private within the chosen participants. Only those selected participants can see the activities in the blockchain. It uses a set of collective admins, i.e.; a set of identifiable entities are defined as miners and all the validation/mining task will be done by them only. But the mining process doesn't involve the proof- of-work (PoW) scheme. Many blockchain networks including bitcoin use PoW scheme, in which a is a piece of data is created to verify the transaction which is difficult to produce but easy for others to verify In Multichain, all the transactions between two participants are secured with a handshaking mechanism. In which a handshaking message and acknowledgment message is used to make sure that the exact participants are available on the communication channel. Following steps will take place between two participants before starting a trans- action

- Each node submits its identity as a public address in a permitted list.
- Each node will verify that the other nodes address is there in its permitted list
- Each node will send a challenge message to the other node.
- After receiving the challenge message each node will send back a signature of the challenge message providing their ownership of the private key corresponding to the public key. If the node who sent the challenge message received a signature message then the transaction between those two participants will start. And if a satisfying signature is not received then the peer to peer connection between those two nodes will disconnect.

### Mining

Multichain introduces a new parameter called 'mining diversity' for defining the mining process. The mining diversity is used for defining the participation of minors in the mining process. In Multichain, mining is done in a "Round-robin schedule". The minors can create valid blocks in a round robin fashion so that all the minors can participate in the mining process equally.

The mining diversity is defined as

“ $0 \leq \text{Mining Diversity} \leq 1$ ”

The ‘1’ represents that every permitted miner will participate in the round robin rotation and ‘zero’ represents no restrictions in mining. All miners can equally participate in the mining process and the validity of the block can be verified through different steps.

In a Multichain platform, there is no transaction cost or block rewards by default. But we can define those parameters in the params.dat file. The params.dat file contains several parameters for defining the blockchain behavior. There is an agricultural supply chain application already available on the Multichain platform. The app can control the entire supply chain system starting from the farmer to the customer. Each stage can be tracked through blockchain and the approach will help to increase the quality, reach and profitability of the product.

---

---

## HydraChain

HydraChain is an open source blockchain platform, which is developed by Brainbot technologies and Ethereum project. HydraChain is an extension of the Ethereum Blockchain platform which provides support to create private/permissioned Blockchain networks. The supporting language for HydraChain is python. As an extension of Ethereum, HydraChain is fully compatible with all the API level and contract level protocols in Ethereum. There are several well-defined tools in Ethereum for creating smart contracts and DApps, (Decentralized Apps). You can reuse all those tools in HydraChain also. So it will be easy for those who know Ethereum to move on to HydraChain.

### Smart contracts and HydraChain

Solidity/Serpent based smart contracts can co-exist in the same chain with the Python based smart contracts. Yes...! They are interoperable. Smart contracts created using HydraChain is independent of EVM (Ethereum virtual machine) as it is developed in Python programming language. The EVM provides a runtime environment for the contracts. EVM will execute all the untrusted codes and can provide security by restricting the accessing of each other’s state. But Python based smart contracts will bypass the EVM so that the contract execution is fast. And we know, python is an easy to use language, less time consuming and easier to debug too. In fact, you don’t need to go for a new language like solidity for developmental purpose.

### How blocks are added?

Basically, HydraChain is providing the permissioned network creation services. So the validation is a great concern here. There will be a registered accountable validators in the network who is responsible for the validation of the blocks and transactions. In a HydraChain network, all the blocks are not allowed to enter the network without validation. That means a block will be added to the network only when the validators sign that the block is required. So once a block is entered into a network it is persistent. There are no reverts.

The HydraChain keeps a limitation in creating the blocks. HydraChain will create a new block if and only if there is a pending transaction. Whenever the Blockchain is unable to hold a transaction then it will create

new block and validator has to sign it as a required block. The block will be added to the network after validation. As the validators are registered, a KYC is used for the participants, to make sure that the transactions take place between registered participants only. The HydraChain platform provides a customizable nature in different components of Blockchain like transaction cost, gas limits, genesis allocation and block time. All these components have an inevitable role in a blockchain.

### **Transaction cost**

The transaction cost in a HydraChain is the cost required for executing the computational steps in a transaction. In the HydraChain, you have the provision to configure the cost as per your requirement. The transaction cost can be calculated using an equation i.e.;  $\text{Transaction cost} = \text{Gas unit} * \text{Gas price}$ .

### **Gas limits**

The gas units are the basic units for an executed transaction in a Blockchain. A transaction can be divided into several 'opcode' and each opcode will have a specific number of gas units based on the type of the opcode. A 'zerostep' opcode has '0' gas units, 'quickstep' opcode has 2 gas units and a 'faststep' opcode has 5 gas units and so on. When a transaction is executing in a blockchain first it will extract the opcodes from the transaction, then the number of gas units will be identified from it, now the gas price will multiply with the total gas units, and that will be the transaction cost for that particular transaction. In HydraChain you can customize the gas limit also. Where the gas limits are the maximum number of computational steps in a transaction. For example: If a blockchain has a gas limit 50 then each transaction should have maximum 50 gas units.

### **Genesis Allocation in HydraChain**

The genesis allocation is related to the hashing and mining capacity of a blockchain. The HydraChain has the power to customize its genesis allocation.

Usually, a Blockchain provides two types of mining methods they are direct mining and indirect mining. In Ethereum you will be using the cryptocurrency 'ether' for financial transactions. While creating a HydraChain you have the provision to decide whether to perform direct mining or indirect mining. Cryptocurrencies like ETH and ETC can be mined directly. And for other currencies like bitcoin, zeta coin etc. you can define an indirect mining with the help of sha256 hashing algorithm. In indirect mining, first you have to mine the Ethereum anyway, at payout time the ETH will exchange with other currencies of your choice at the latest exchange rate. This customization feature in mining will provide a facility to do financial transaction with all currencies.

### **Block time**

One more customization is possible in HydraChain that is block time. Block time is the time delay between the validations of two blocks. An average block time in a Bitcoin Blockchain is 10 minutes that means it will take 10 minutes for the addition of a new block to a Blockchain.

---

---