

MultiChain 1.0.4

 MultiChain	Permissioned Blockchain	
	Systeemvereisten:	Linux/Windows/Mac
	Ontwikkeld door:	Coin Sciences Ltd
GPLv3 (Open Source)	Contactpersoon:	Kristof.Verslype@Smals.be

Functionaliteiten

MultiChain is een blockchain technologie die toelaat om zelf permissioned (afgeschermd, private) blockchain netwerken op te zetten, te beheren en erin te participeren. Elke participant (node) in het afgeschermd blockchain netwerk zal de software moeten draaien.

Blockchain technologie kun je gebruiken voor 1) het beschermen van gegevens, 2) het transfereren van activa en 3) het afdwingen van regels (d.m.v. smart contracts). MultiChain ondersteunt enkel de eerste twee aspecten. Het is een relatief eenvoudige technologie, wat ook een aantal voordelen heeft. Ten eerste is MultiChain erg stabiel en ten tweede kan erg snel een effectief gedistribueerd netwerk opgezet worden. Die stabiliteit komt deels voort uit het feit dat MultiChain een fork is van de code van Bitcoin, de meest geteste blockchain technologie. Dit geeft ons ook meer vertrouwen in de correctheid van de code.

Via *data streams* kan data in de blockchain bewaard en doorgegeven worden. MultiChain laat toe om verschillende types tokens, die typisch activa representeren, aan te maken en te transfereren. Het biedt *multisig* ondersteuning, wat betekent dat een transactie enkel geldig is indien het door voldoende entiteiten ondertekend wordt. Een transactie kan vb. vereisen dat twee uit een set van drie entiteiten meewerken. Dit laat op zijn beurt toe dat bij één transactie meerdere activa tegelijkertijd van eigenaar veranderen (swaps). Het rechtenbeheer is flexibel en kan gecentraliseerd of gedecentraliseerd gebeuren. In dat laatste geval is er een stemronde onder de beheerders. Heel wat parameters kunnen geconfigureerd worden voorafgaandelijk aan het lanceren van de blockchain. MultiChain mist wel modulariteit. Zo is het niet mogelijk om een andere onderliggende database dan LevelDB te gebruiken.

Conclusies & Aanbevelingen

MultiChain laat toe om snel tot concrete resultaten te komen en is bovendien vrij efficiënt. Anderzijds mankeert het ondersteuning van smart contracts. Het product geeft technisch de indruk dat er zelfs al voorzichtig zaken mee in productie gebracht kunnen worden. Zorg wel goed voor je private sleutels in je wallet. Hou er ook rekening mee dat de blockchain technologie in het algemeen nog in volle ontwikkeling is, en dat we dus ook voor MultiChain niet weten of het binnen een paar jaar nog zal bestaan of relevant zal zijn. Een daarmee gerelateerd risico bij Multichain is zijn relatief kleine ontwikkel community.

Testen & Resultaten

De MultiChain website oogt vrij rudimentair, maar bevat alle nodige informatie om snel aan de slag te gaan. Er zijn verschillende, makkelijk te volgen tutorials (die effectief werken) en die samen een vrij volledig beeld geven wat er mogelijk is.

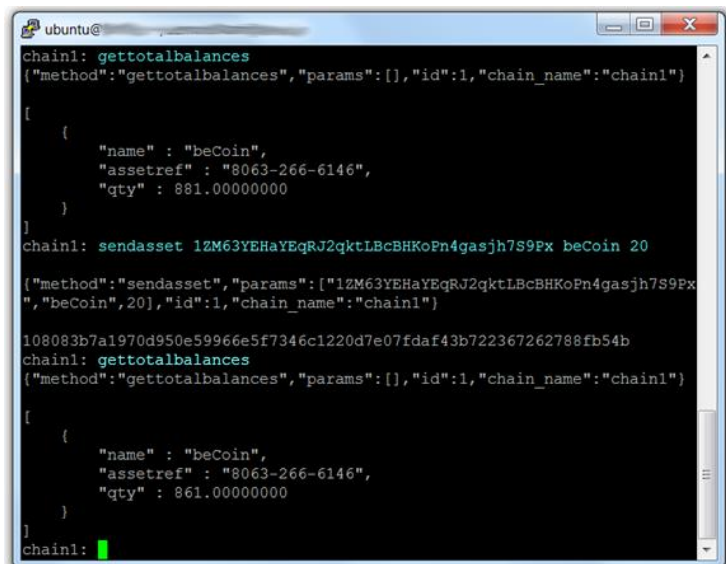
Vooraleer je begint zijn er heel wat parameters die je kunt kiezen zoals de frequentie voor de creatie van nieuwe blokken, de maximale bloksgrootte, het percentage van de admins dat moet akkoord zijn om een node mee in te laten staan voor het collectief veilig houden van de blockchain, ...

We hebben in een cloud omgeving een blockchain netwerk opgezet met vier Ubuntu machines. Drie daarvan hadden admin rechten. Een in onze lokalen opgezette vijfde machine werd toegevoegd, kreeg bepaalde rechten, en werd, ten slotte, weer verwijderd. Dit vereiste telkens het akkoord van de meerderheid van de admins. Een node kan participeren in meerdere blockchain netwerken.

Onze proof of concept maakt gebruik van *data streams* om data op de blockchain te bewaren. Deze data werd in *multisig* transacties gestoken en door twee participanten ondertekend. In de praktijk betekende dit dat partij A een transactie ondertekent en voorstelt aan partij B. Na de nodige verificaties plaatst ook partij B zijn handtekening en publiceert het de transactie op de blockchain. We hebben de data stream zo geconfigureerd dat enkel bepaalde *multisig* transacties aanvaard worden.

Het aanmaken en transfereren van tokens was niet vereist in de PoC en werd dus maar in beperktere mate getest (zie figuur 1). Voor de performantie baseren we ons voorlopig op cijfers op de MultiChain website, waar wordt gesteld dat duizend transacties per seconde verwerkt kunnen worden. Dit aspect willen we nog zelf testen.

Voor onze PoC keken we initieel naar smart contract technologieën, maar bij nader inzien waren *multisig* transacties beter geschikt. Dit resulteerde in een snellere ontwikkeling en hogere efficiëntie en stabiliteit. MultiChain weet wat ze wil. De mogelijkheden zijn beperkt in vergelijking met smart contract technologieën, maar dat wat ze aanbiedt werk wel zoals het hoort.



```
ubuntu@
chain1: gettotalbalances
{"method": "gettotalbalances", "params": [], "id": 1, "chain_name": "chain1"}
{
  {
    "name": "beCoin",
    "assetref": "8063-266-6146",
    "qty": 881.00000000
  }
}
chain1: sendasset 12M63YEHaYEqRJ2qktLbCBHkoPn4gasjh7S9Px beCoin 20
{"method": "sendasset", "params": ["12M63YEHaYEqRJ2qktLbCBHkoPn4gasjh7S9Px", "beCoin", 20], "id": 1, "chain_name": "chain1"}
108083b7a1970d950e59966e5f7346c1220d7e07fdaf43b722367262788fb54b
chain1: gettotalbalances
{"method": "gettotalbalances", "params": [], "id": 1, "chain_name": "chain1"}
{
  {
    "name": "beCoin",
    "assetref": "8063-266-6146",
    "qty": 861.00000000
  }
}
chain1: █
```

Figuur 1. Via het commando *gettotalbalances* zie ik dat ik over 881 beCoins beschik. Ik transfereer er met het commando *sendasset 20* en hou er nog 861 over.

Gebruiksvoorwaarden & Budget

MultiChain is open source (GPLv3) en is dus gratis te downloaden en te gebruiken. Coin Sciences Ltd, het bedrijf achter MultiChain, alsook haar platforms partners bieden professionele ondersteuning aan.