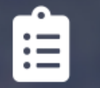
ETHEREUM

UNE PLATEFORME INFORMATIQUE DÉCENTRALISÉE BASÉE SUR LA BLOCKCHAIN


Une blockchain


Une plateforme *smart contracts*


Un langage

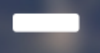

Des outils de développement


Le frontend


Des infrastructures


Des outils de debug et de tests


Avantages


Limitations


Le futur

LA BLOCKCHAIN : UN REGISTRE PUBLIC, ANONYME ET INFALSIFIABLE

- Registre des transations : un fichier qui contient toutes les informations depuis le premier bloc
- Théories des jeux : l'ensemble de règles de consensus
- P2P: un réseau de noeuds parlant le protocole et gardant une trace des transactions
- TCP/IP : l'infrastructure Internet

LA BLOCKCHAIN : UN REGISTRE PUBLIC, ANONYME ET INFALSIFIABLE

UN PEU DE CRYPTO : LES ADRESSES EOA

- Clé privée de 32 octets
- Clé publique ECDSA 512
- Addresse dérivée de la clé publique (20 derniers octets de l'empreinte Keccak-256)

LA BLOCKCHAIN : UN REGISTRE PUBLIC, ANONYME ET INFALSIFIABLE

UNE CHAÎNE IMMUTABLE

- Chaque "full node" a une copie de la chaîne.
- Chaque bloc a un espace de stockage limité.
- Chaque bloc contient le hash du bloc précédent.
- Une modification malicieuse de la chaîne provoque l'exclusion du noeud incriminé.
- Difficulté (impossibilité) de modifier l'information.

BEST BLOCK
#5,625,309

UNCLES (CURRENT / LAST 50)
0/0

LAST BLOCK
12 s ago

AVG BLOCK TIME
15.31 s

AVG NETWORK HASHRATE
0.2 H/s

DIFFICULTY
0.00 H

ACTIVE NODES 39/40

GAS PRICE 10 gwei

GAS LIMIT 7992222 gas

PAGE LATENCY 154 ms

UPTIME 100%

BLOCK TIME

DIFFICULTY

BLOCK PROPAGATION

LAST BLOCKS MINERS

UNCLE COUNT (25 BLOCKS PER BAR)

TRANSACTIONS

GAS SPENDING

GAS LIMIT

ATTENTION!

This page does not represent the entire state of the ethereum network - listing a node on this page is a voluntary process.

Astatium		107 ms		133	164	#5,625,309	0e5e7f09...59c4cbd4	4.231638674403815e+21	92	0	13 s ago	0 ms		9 days	100%
ethpool.maxhash.org (AS)	Parity//v1.8.11-stable-21522ff-20180227/x86_64-linux-gnu/rustc1.24.0	137 ms	0 KH/s	120	104	#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	54	0	15 s ago	0 ms		9 days	100%
CIMS FARM CRYPTO. INVEST.	Geth/v1.8.2-stable-b8b9f7f4/linux-amd64/go1.9.4	1 ms		147	1113	#5,625,309	0e5e7f09...59c4cbd4	4.231638674403815e+21	92	0	12 s ago	+122 ms		9 days	100%
ethpool.maxhash.org (EU)	Geth/v1.8.7-stable-66432f38/linux-amd64/go1.10.1	45 ms	0 KH/s	86	107	#5,625,309	0e5e7f09...59c4cbd4	4.231638674403815e+21	92	0	12 s ago	+192 ms		9 days	100%
ethpool.maxhash.org (US)	Parity//v1.8.11-stable-21522ff-20180227/x86_64-linux-gnu/rustc1.24.0	8 ms	0 KH/s	142	60	#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	54	0	15 s ago	+231 ms		9 days	100%
Foundation Monitoring (Experimental-master)	Geth/v1.8.8-unstable-7beccb29/linux-amd64/go1.9.4	38 ms		25	4919	#5,625,309	0e5e7f09...59c4cbd4	4.231638674403815e+21	92	0	14 s ago	+364 ms		9 days	100%
ethpool.maxhash.org (US2)	Geth/v1.8.2-stable/linux-amd64/go1.9.2	8 ms	0 KH/s	78	71	#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	54	0	14 s ago	+499 ms		9 days	100%
WORLES COMMON	Geth/v1.8.7-stable-66432f38/windows-amd64/go1.10.1	47 ms		12	0	#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	0	0	14 s ago	+727 ms		9 days	100%
[Universa Blockchain] geth-mainnet-3	Geth/v1.8.6-stable/linux-amd64/go1.10.1	5 ms		69	5079	#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	54	0	14 s ago	+1.2 s		9 days	100%
iit-02 iit.edu		11 ms		28	642	#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	54	0	14 s ago	+1.2 s		9 days	100%
Zetabit2	Parity//v1.9.6-stable-df92977-20180416/x86_64-linux-gnu/rustc1.25.0	49 ms		72	0	#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	54	0	14 s ago	+1.3 s		9 days	100%
Foundation Monitoring (Develop)	Geth/v1.8.6-unstable-16a78b09/linux-amd64/go1.10.1	37 ms		48	4811	#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	54	0	13 s ago	+1.6 s		9 days	100%
iit-01 iit.edu		11 ms		27	559	#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	54	0	13 s ago	+1.7 s		9 days	100%
Foundation Monitoring (Experimental-fastsync)	Geth/v1.8.8-unstable/linux-amd64/go1.10.2	37 ms		25	4836	#5,625,309	0e5e7f09...59c4cbd4	4.231638674403815e+21	92	0	13 s ago	+1.7 s		9 days	100%
kinΞTH-light		73 ms		15	54	#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	54	0	13 s ago	+2.0 s		9 days	100%
veox-geth-lightserv	Geth/v1.8.7-stable-66432f38/linux-amd64/go1.10	59 ms		701	2972	#5,625,309	0e5e7f09...59c4cbd4	4.231638674403815e+21	92	0	11 s ago	+3.0 s		9 days	100%
BanditCountry	Parity//v1.9.1-beta-aca9f13-20180201/x86_64-linux-gnu/rustc1.23.0	84 ms		19	0	#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	54	0	12 s ago	+3.1 s		9 days	100%
kinΞTHity	Parity//v1.10.2-beta-f4ae813-20180423/x86_64-linux-gnu/rustc1.25.0	53 ms		13	0	#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	54	0	11 s ago	+3.6 s		9 days	100%
arcturus	Parity//v1.11.1-beta-6654d02-20180515/x86_64-linux-gnu/rustc1.25.0	45 ms		221		#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	54	0	10 s ago	+4.7 s		9 days	100%
Bootnode-BR	Geth/v1.8.7-stable/linux-amd64/go1.10.2	59 ms		271	4903	#5,625,309	0e5e7f09...59c4cbd4	4.231638674403815e+21	92	0	8 s ago	+6.2 s		9 days	100%

UNE PLATEFORME SMART CONTRACTS

- Smart contracts : des opérations plus compliquées que des simples transactions
- Registre des transations : un fichier qui contient toutes les informations depuis le premier bloc
- Théories des jeux : l'ensemble de règles de consensus
- P2P: un réseau de noeuds parlant le protocole et gardant une trace des transactions
- TCP/IP : l'infrastructure Internet

UNE PLATEFORME SMART CONTRACTS

- Contract Account, code machine sur la blockchain.
- Ethereum virtual machine, sur tous les noeuds.
- Turing complet, déterministe, isolée.
- Instructions exécutées par tous les noeuds.
- Notion de gaz pour inciter à l'optimisation, empêcher les exécutions trop longues et rémunérer les mineurs.
- Gaz == ETH. Paiement des utilisateurs de la plateforme aux machines exécutant les requêtes.
- Plusieurs clients : geth, parity, cpp-ethereum, …

UN LANGAGE : SOLIDITY

```
pragma solidity ^0.4.22;
/* Un langage objet */
contract Mortal {
    address owner;

    constructor() public { owner = msg.sender; }
    function kill() public { if (msg.sender == owner) selfdestruct(owner)
}

/* De l'héritage */
contract AramisGreeter is Mortal {
    string private greeting;

    constructor() public {
        greeting = "10ème journée - Aramis 2018" ;
    }

    function greet() public constant returns (string) {
        return greeting;
    }
}
```

DES OUTILS DE DÉVELOPPEMENT

- Processus complexe, nombreuses étapes.
- Contrats non modifiables après déploiement.
- Truffle, framework de développement.
- Compilations, Migrations, déploiements, tests, package management.

LE FRONTEND

Du javascript : web3.js

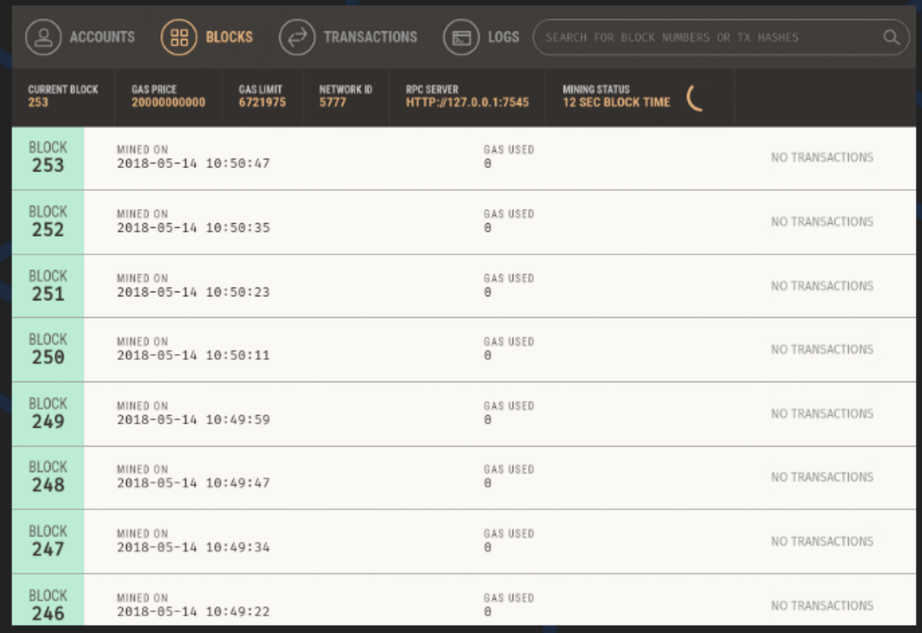
```
var Web3 = require('web3');
web3 = new Web3(new Web3.providers.HttpProvider(" https://mainnet.

abi=[{"constant":false,"inputs":[],"name":"kill","outputs":[],"pay

var AramisGreeter = web3.eth.contract(abi);
var myContractInstance = MyContract .at('0xa317e1e75379CCab2451d7a
var greet = myContractInstance .greet.call();

document.getElementById('greet').innerText = greet;
```

```
<span id="greet"><span>
```

DES OUTILS DE DEBUG ET DE TESTS

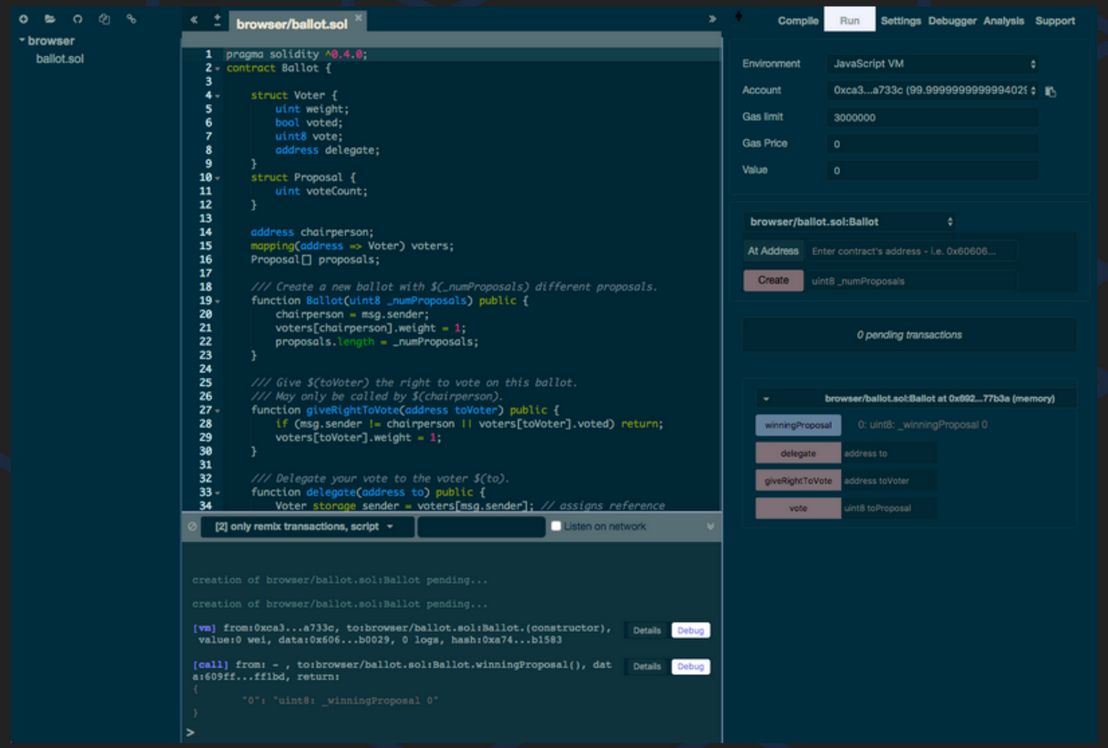
TRUFFLE :

- framework de test (en JS ou Solidity).
- debugger.
- chaînes de test locales : testrpc, ganache.



DES OUTILS DE DEBUG ET DE TESTS

Remix IDE et debugger https://remix.ethereum.org



DES OUTILS DE DEBUG ET DE TESTS

CHAÎNES DE TESTS

- ropsten
- rinkeby/kovan

DES INFRASTRUCTURES

- 15000 noeuds
- Pas forcément la possibilité de faire tourner un noeud, Infura
- Etherscan

✚ AVANTAGES

- véritable décentralisation
- réseau résilient
- open source
- gouvernance
- très forte communauté
- dynamisme

— LIMITATIONS

- défauts de jeunesse
- bugs: DAO et Parity Multiwallet * 2
- POW
- lent : 8-10 tx/seconde, ~800000 tx/jour
- points faibles: DNS et hébergement
- un nouveau langage à apprendre
- spéculation et bruit !

LE FUTUR

- évolutions du protocole : casper, sharding
- state channel : µraiden et raiden
- chaîne fille : plasma
- ENS, IFPS, swarm,
- un nouveau langage: vyper

MERCI !

- yellow paper (Gavin Wood)
- Vitalik Buterin's website
- etherscan, infura
- contract Aramis
- https://huit.re/aramis-ethereum