



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 transactions : 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

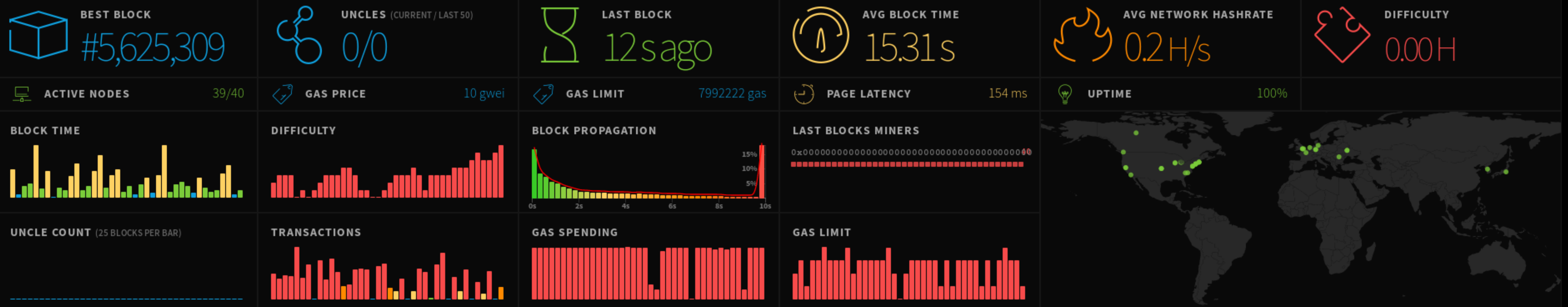
- Clé privée de 32 octets
- Clé publique ECDSA 512
- Adresse dérivée de la clé publique (20 derniers octets de l'empreinte Keccak-256)

■ 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.










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

Node Name	Software	Latency	Uptime	Block Count	Gas Price	Block Hash	Peer ID	Latency	Uptime	Block Time	Block Age	Block Time	Uptime	
Astatium		107 ms	133	164	#5,625,309	0e5e7f09...59c4cbd4	4.231638674403815e+21	92	0	13 s ago	0 ms	[Bar chart]	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	[Bar chart]	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	[Bar chart]	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	[Bar chart]	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	[Bar chart]	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	[Bar chart]	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	[Bar chart]	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	[Bar chart]	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	[Bar chart]	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	[Bar chart]	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	[Bar chart]	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	[Bar chart]	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	[Bar chart]	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	[Bar chart]	9 days 100%	
kinETH-light		73 ms	15	54	#5,625,309	484de7cb...f709ae96	4.231638674403815e+21	54	0	13 s ago	+2.0 s	[Bar chart]	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	[Bar chart]	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	[Bar chart]	9 days 100%	
kinETHity	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	[Bar chart]	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	[Bar chart]	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	[Bar chart]	9 days 100%	

UNE PLATEFORME SMART CONTRACTS

-  Smart contracts : des opérations plus compliquées que des simples transactions
-  Registre des transactions : 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;
    }
}
```



```
Compile:      truffle compile
Migrate:     truffle migrate
Test contracts: truffle test
~/t/a/aramis-ethereum-contract truffle create contract AramisGreeter 2051ms < dim. 13 mai 2018 16:21:32 CEST
~/t/a/aramis-ethereum-contract vi contracts/AramisGreeter.sol 628ms < dim. 13 mai 2018 16:21:39 CEST
~/t/a/aramis-ethereum-contract vi migrations/2_deploy_contracts.js 5.7s < dim. 13 mai 2018 16:21:52 CEST
~/t/a/aramis-ethereum-contract vi truffle.js 7.5s < dim. 13 mai 2018 16:22:05 CEST
~/t/a/aramis-ethereum-contract truffle compile 15.6s < dim. 13 mai 2018 16:22:25 CEST
```

```
(node:3722) ExperimentalWarning: The fs.promises API is experimental
Compiling ./contracts/AramisGreeter.sol...
Compiling ./contracts/Migrations.sol...
```

Compilation warnings encountered:

```
/home/remche/taf/aramis/aramis-ethereum-contract/contracts/Migrations.sol:13: Warning: Defining constructors as functions with the same name as the contract is deprecated. Use "constructor(...) { ... }" instead.
function Migrations() public {
^ (Relevant source part starts here and spans across multiple lines).
```

Writing artifacts to ./build/contracts

```
~/t/a/aramis-ethereum-contract truffle console --network ropsten 3504ms < dim. 13 mai 2018 16:22:37 CEST
```

```
(node:3765) ExperimentalWarning: The fs.promises API is experimental
truffle(ropsten)> deploy
Using network 'ropsten'.
```

Running migration: 1_initial_migration.js

Deploying Migrations...

... 0x6a717faf46a21578e74b8e5043e4ba37222484d57ff7706d501a051bcb4adb35

Migrations: 0xaee5071491e400902e11f907205d97f1c485

Saving successful migration to network...

... 0xa8ef9d427b495698ff983aedbcb2c14165b0fc87f718edf096a88a354f1dbef5

Saving artifacts...

Running migration: 2_deploy_contracts.js

Deploying AramisGreeter...

... 0xd50eb2e90e4bccbcef777e9f743fdb196c7853e69475d97e59119088be132f94

AramisGreeter: 0xa317ele75379ccab2451d7a506dde86763fe5c86

Saving successful migration to network...

... 0xcc97594f4eef73d475820cbelea3f7f0d66a28e1c58a50194a7256e58f7b7365

Saving artifacts...

truffle(ropsten)> AramisGreeter.address

'0xa317ele75379ccab2451d7a506dde86763fe5c86'

truffle(ropsten)> AramisGreeter.deployed().then((instance) => {app=instance})

undefined

truffle(ropsten)> app.greet()

'10ème journée - Aramis 2018'

truffle(ropsten)>

- 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;
```

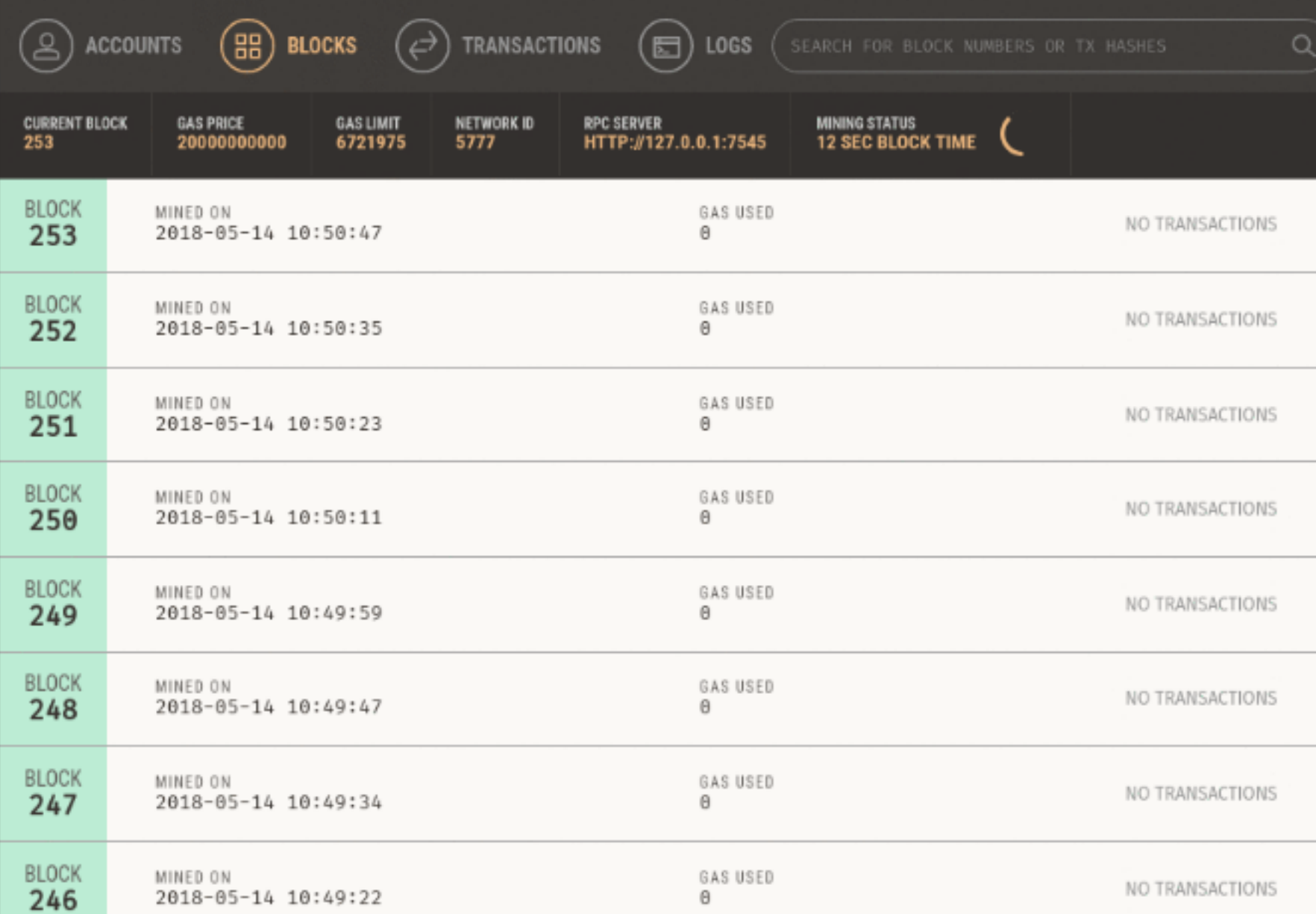
```
<span id="greet"><span>
```



DES OUTILS DE DEBUG ET DE TESTS

TRUFFLE :

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

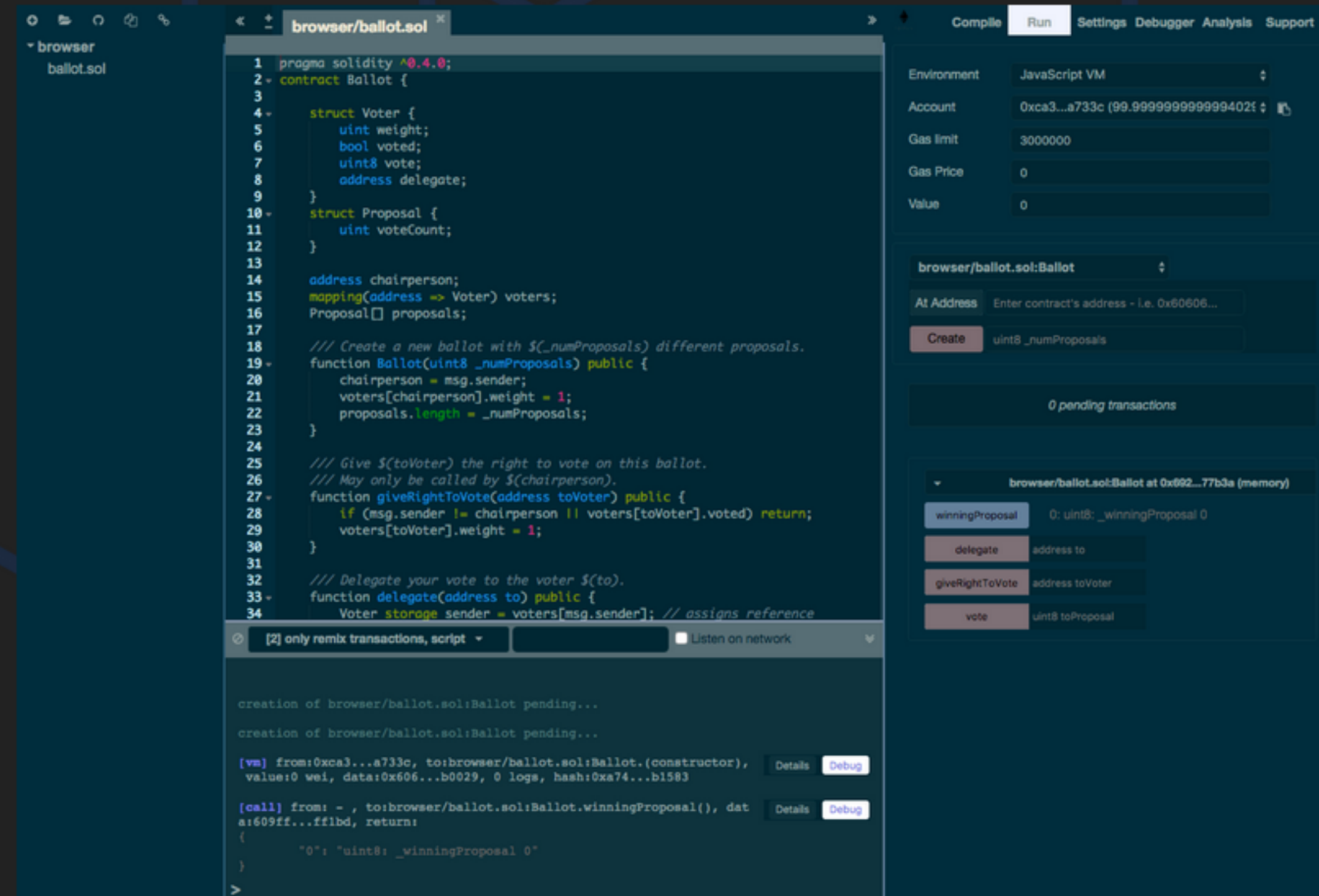


The screenshot shows the 'BLOCKS' tab in the Truffle interface. The top navigation bar includes 'ACCOUNTS', 'BLOCKS', 'TRANSACTIONS', and 'LOGS'. A search bar is present with the text 'SEARCH FOR BLOCK NUMBERS OR TX HASHES'. Below the navigation, a summary bar displays: 'CURRENT BLOCK 253', 'GAS PRICE 20000000000', 'GAS LIMIT 6721975', 'NETWORK ID 5777', 'RPC SERVER HTTP://127.0.0.1:7545', and 'MINING STATUS 12 SEC BLOCK TIME'. The main content is a table of mined blocks.

BLOCK	MINED ON	GAS USED	TRANSACTIONS
253	2018-05-14 10:50:47	0	NO TRANSACTIONS
252	2018-05-14 10:50:35	0	NO TRANSACTIONS
251	2018-05-14 10:50:23	0	NO TRANSACTIONS
250	2018-05-14 10:50:11	0	NO TRANSACTIONS
249	2018-05-14 10:49:59	0	NO TRANSACTIONS
248	2018-05-14 10:49:47	0	NO TRANSACTIONS
247	2018-05-14 10:49:34	0	NO TRANSACTIONS
246	2018-05-14 10:49:22	0	NO TRANSACTIONS

DES OUTILS DE DEBUG ET DE TESTS

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



The screenshot displays the Remix IDE interface. The main editor shows Solidity code for a `Ballot` contract. The code includes a `pragma solidity ^0.4.0;` declaration, a `contract Ballot {` block, and several functions: `Ballot(uint8 _numProposals)` for creating a ballot, `giveRightToVote(address toVoter)` for granting voting rights, and `delegate(address to)` for delegating votes. The contract uses `struct` for `Voter` and `Proposal`, and a `mapping` for `voters`.

The right-hand panel shows the environment settings (JavaScript VM, Account: `0xca3...a733c`, Gas limit: `3000000`) and the `browser/ballot.sol:Ballot` contract instance. The instance has a `Create` button and a `uint8 _numProposals` input field. Below the instance, there are buttons for `winningProposal`, `delegate`, `giveRightToVote`, and `vote`.

The bottom panel shows the transaction log, including the creation of the `Ballot` contract and a call to `winningProposal()` returning `uint8: _winningProposal 0`.



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 : μ raiden 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>