ÉTUDE DE LA CONSOMMATION ÉNERGÉTIQUE DES SMART CONTRACTS DANS LA BLOCKCHAIN ETHEREUM

Jean-Patrick Gelas, Hayri Acar, Hind Benfenatki
Université Lyon 1/LIRIS/INRIA/ENS Lyon

Entretiens Jacques Cartier, 12-13 novembre 2018, ENS Lyon

jp@ejc2018:~$ whoami

```
{
    "first_name" : "Jean-Patrick",
    "last_name" : "Gelas",
    "job" : "Assistant Professor",
    "locations" : [ "Université Claude Bernard - Lyon 1",
            "Avalon/INRIA/ENS Lyon" ],
    "url" : "https://perso.univ-lyon1.fr/jean-patrick.gelas",
    "email" : "jean-patrick.gelas@univ-lyon1.fr",
    "github" : "https://github.com/jpgelas",
    "hobbies" : [ "skydive", "wingsuit" ]
}
```

AGENDA

On ne parlera pas de ...

- Cryptographie, Hash, Merkle tree,...
- Algorithmes de consensus (PoW, PoS, DPoS,...)
- Plateformes d'échanges
- Comment miner de la crypto monnaie
- Comment devenir crypto millionaire ! ☺

COMPARATIF

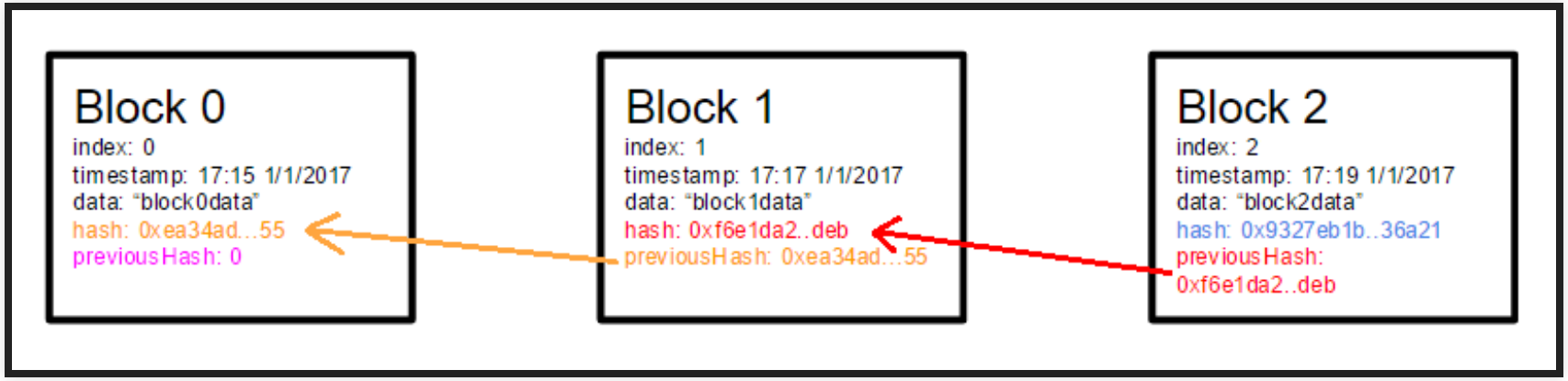
	Yearly Cost	Energy Used (GJ)
Gold Mining	$105B	475M
Gold Recycling	$40B	25M
Paper Currency and Minting	$28B	39M
Banking System	$1,870B	2,340M
Governments	$27,600B	5,861M
Bitcoin Mining	$4.5B	183M

https://blog.picks.co/pow-is-efficient-aa3d442754d3

OBJECTIFS

- Rappels (Blockchain, Mineurs, ...)
- Introduction à la blockchain **Ethereum**
- Les Smart Contracts : Création, déploiement, fonctionnement.
- Modélisation et maîtrise de leur consommation.

BLOCKCHAIN



- Blockchain : Structure de données simple
- La technologie Blockchain : « Base de données » sécurisées et décentralisées.

Démo : https://anders.com/blockchain/

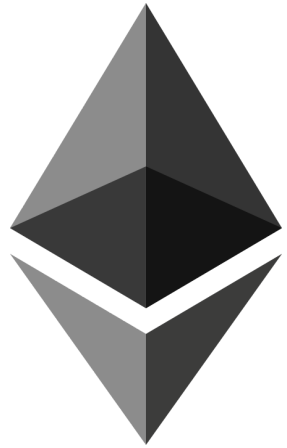
LES MINEURS

- Héberge une copie de la blockchain
- Ajoutent de nouvelles liste de transactions (*i.e.* des blocs) à la chaîne.
- Vérifient l'intégrité de la blockchain
- Génèrent de nouveaux *coins*
- (Exécutent les Smart Contracts)

ETHEREUM

> *Protocole d'échanges décentralisés permettant la création par les utilisateurs de contrats intelligents grâce à un langage Turing-complet.*
>
> *- Wikipedia*

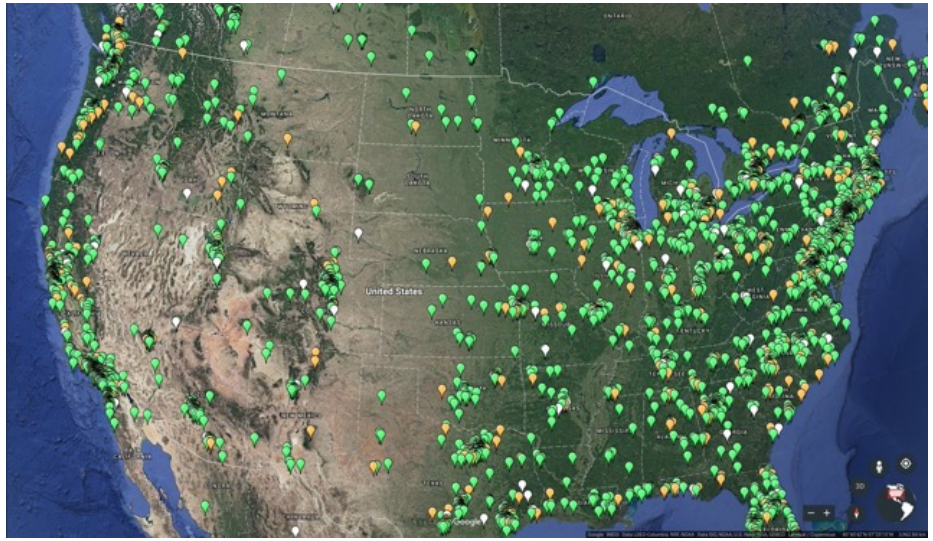
ETHEREUM

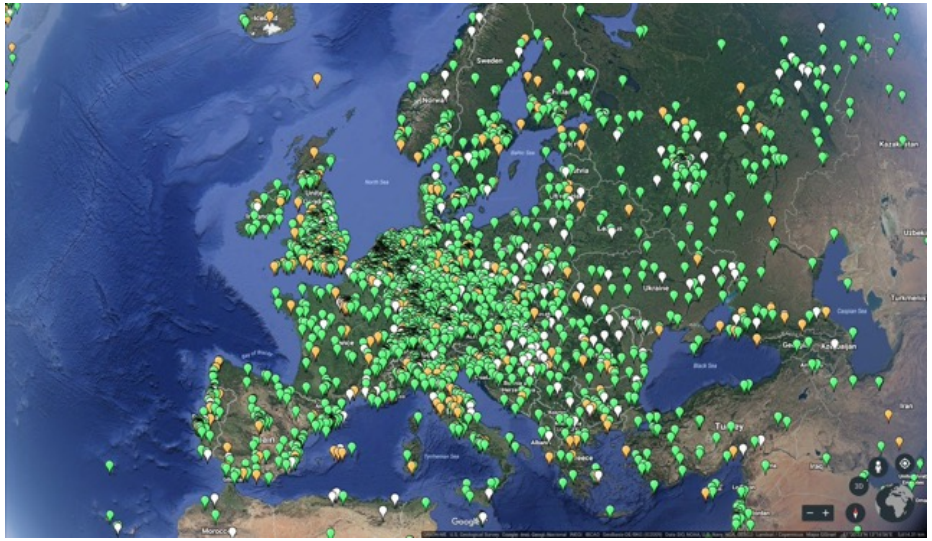


- Blockchain de *seconde génération*
- Développée par *Vitalik Buterin*, lancée en juillet 2015.
- Fréquence moyenne des blocs : 14-15 secondes
- Taille des blocs : dynamique
- Symbole boursier : *ETH*
- Quantité maximale : non limitée

L’infrastructure Ethereum

27500 nœuds contre 7000 pour Bitcoin

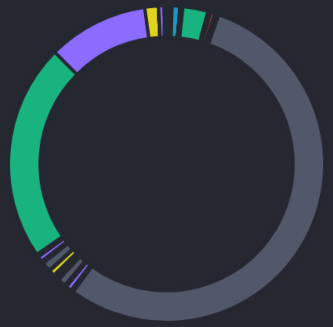




Source: https://twitter.com/peter_szilagyi/status/887272506914213888 - 18/07/2017

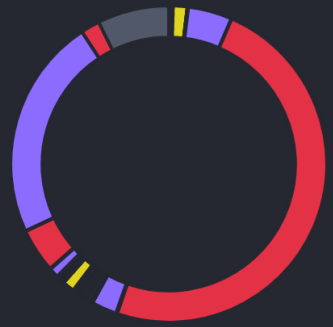
Network number 1 Last updated a few seconds ago

CLIENTS



Clients

Client Versions



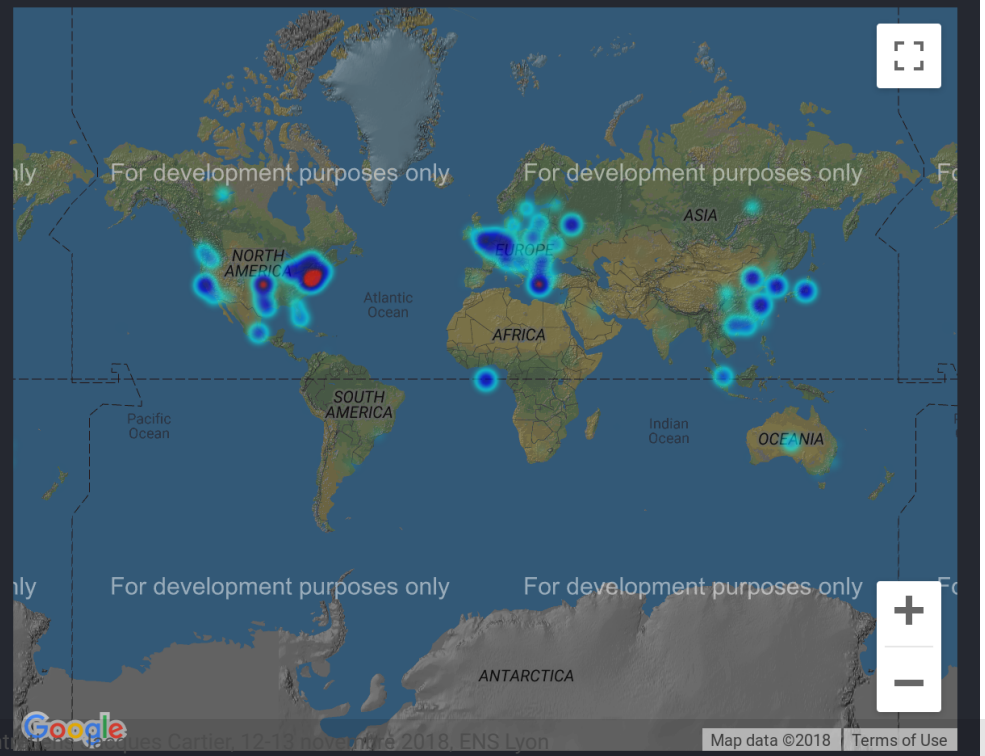
OS

Like what you see? Support the node explorer!

https://www.ethernodes.org

COUNTRIES

Total	13320 (100%)
United States	5738 (43.08%)
China	1639 (12.30%)
Canada	1041 (7.82%)
Germany	587 (4.41%)
Russian Federation	476 (3.57%)
United Kingdom	419 (3.15%)
Netherlands	288 (2.16%)
Korea, Republic of	246 (1.85%)
France	236 (1.77%)
Greece	215 (1.61%)



ethereum

SMART CONTRACT

- Programme autonome
- Déployé et répliqué
- Non modifiable
- Adapté pour gérer des transactions

SMART CONTRACT *SUITE*

- Du *bytecode* stocké dans la blockchain
- Rédigé dans un langage de haut niveau : *Solidity*
- Compilé (*solc*)
- Accessible via une adresse codée sur *160 bits*
- Exécuté dans l'*Ethereum Virtual Machine* (EVM)

0x71c7656ec7ab88b098defb751b7401b5f6d8976f

CODE MACHINE

```
"opcodes": "PUSH1 0x80 PUSH1 0x40 MSTORE
CALLVALUE DUP1 ISZERO PUSH2 0x10 JUMPI PUSH1 0x0
DUP1 REVERT JUMPDEST POP PUSH1 0x40 MLOAD PUSH1
0x20 DUP1 PUSH2 0x487 DUP4 CODECOPY DUP2 ADD
PUSH1 0x40 SWAP1 DUP2 MSTORE SWAP1 MLOAD PUSH1..."
"object":
"608060405234801561001057600080fd5b5060405160
208061048783398101604090815290516000805460016
0a060020a031916331780825560160a060020a031681
526001602081905292902091909155560ff8166100606..."
```

LE LANGAGE SOLIDITY

- Langage de haut niveau
- influencé par C++, Python et Javascript.
- Typé statiquement.
- Supporte l'héritage,
- l'appel à des bibliothèques,
- la définition de type complexe par les utilisateurs.

HELLO WORLD

```
pragma solidity ^0.4.18;
contract Hello {
    string message = "Default message";

    function getMessage () public view returns (string) {
        return message;
    }
    function setMessage (string _message) public payable {
        message = _message;
    }
}
```

0X (ZRX) TOKEN (ERC-20)

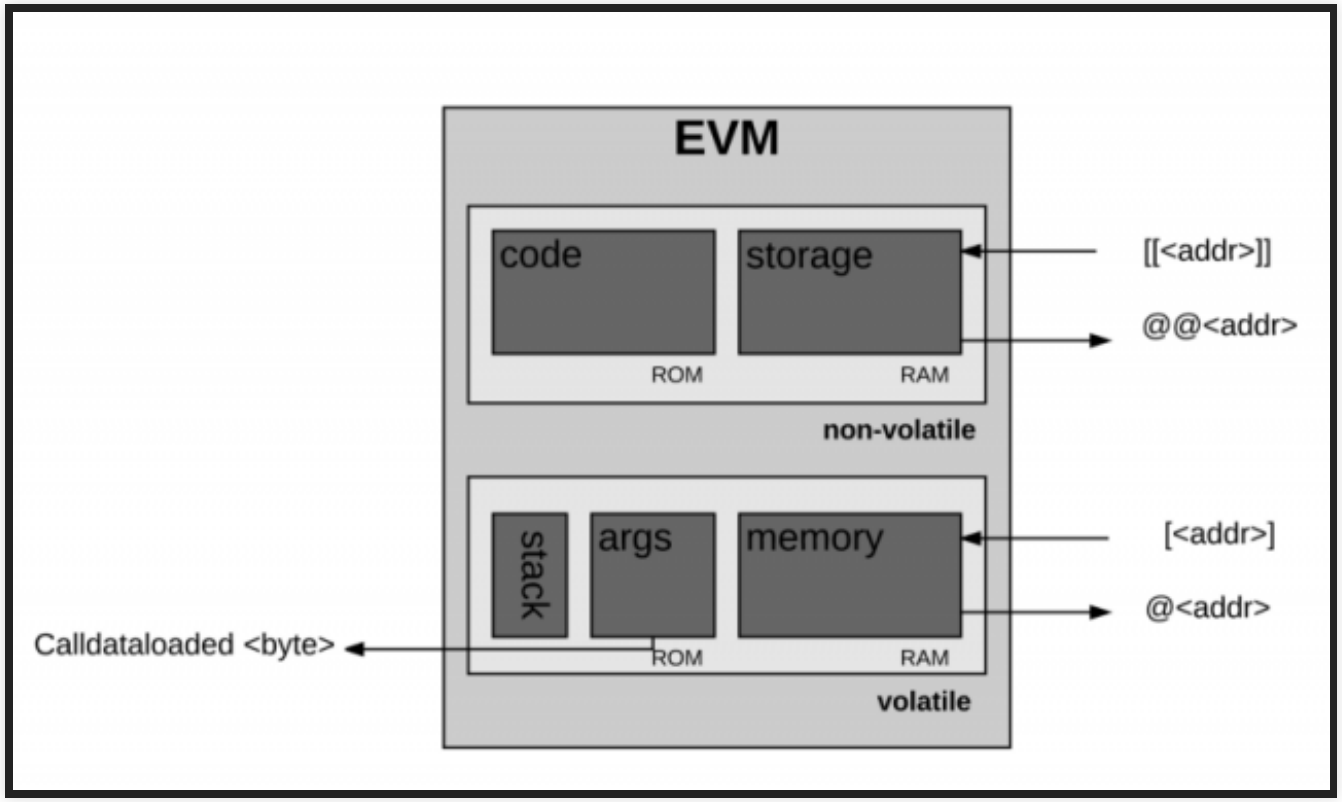
```
contract ZRXToken is UnlimitedAllowanceToken {

    uint8 constant public decimals = 18;
    uint public totalSupply = 10**27; // 1 billion tokens, 18
    string constant public name = "0x Protocol Token";
    string constant public symbol = "ZRX";

    function ZRXToken() {
        balances[msg.sender] = totalSupply;
...
```

NEXIUM (NXC) TOKEN (ERC-20)

```
contract Nexium {
    ...
    function Nexium() {
        initialSupply = 100000000000;
        balanceOf[msg.sender] = initialSupply;
        name = 'Nexium';
        symbol = 'NxC';
        decimals = 3;
        burnAddress = 0x1b320000000000000000000000000000000000
    }
    function totalSupply() returns(uint){
        return initialSupply - balanceOf[burnAddress];
    }
    function transfer(address _to, uint256 _value) ...
    function transferFrom(address _from, ...
```

http://b2expand.com/nexium-token

ETHEREUM VIRTUAL MACHINE



ETHEREUM VIRTUAL MACHINE

- Machine (quasi-) Turing complete.
- Environnement d'exécution des Smart Contracts
- Émule une machine *256 bits* avec des pseudo-registres
- Registres émulés par une *stack* virtuel

ETHEREUM ET UNITÉS DE MESURE

- **Ether** (ETH) : le nom de la crypto monnaie
- **Wei** : une fraction d'Ether (1 ETH = 10^{18} Wei)
- **GAS** : unité de mesure en terme de quantité de calcul
- **GAS price** : défini le prix (en GWei) que vous êtes prêt à payer au mineur.
- **GAS limit** : Quantité maximum de gas que vous êtes prêt à payer pour une transaction.

ANALOGIE

- *GAS limit* : capacité du réservoir d'une voiture en litre.
- *GAS price* le prix du litre de carburant.
  - Voiture : 1,50 EUR (prix) par litre (unité)
  - Ethereum : 20 GWei (prix) par GAS (unité)
- Pour remplir le réservoir il faut :
  - 50 litres à 1,50 EUR = 75 EUR
  - 21000 unités de GAS à 20 GWei = 0.00042 ETH

REMARQUES

- Fixer un *GAS limit* évite de dépenser une fortune en cas de problème.
- La quantité de GAS requise est définie par la quantité d'instructions exécutées.
- Fixer un *GAS limit* trop petit a peu d'intérêt.

COÛT DES INSTRUCTIONS

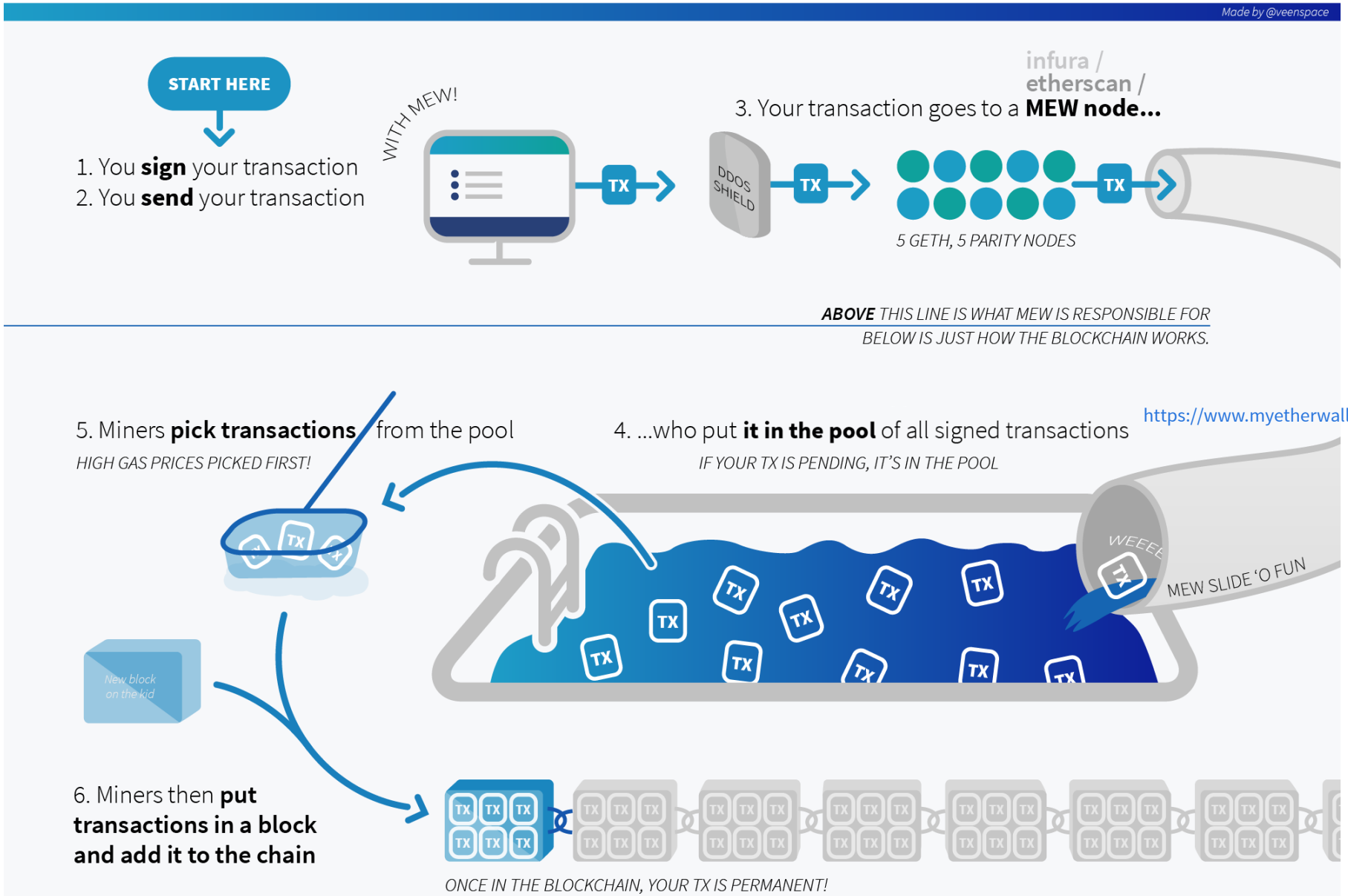
Value	Mnemonic	Gas Used	Subset	Removed from stack	Added to stack	Notes
0x00	STOP	0	zero	0	0	Halts execution.
0x01	ADD	3	verylow	2	1	Addition operation
0x02	MUL	5	low	2	1	Multiplication operation.
0x03	SUB	3	verylow	2	1	Subtraction operation.
0x04	DIV	5	low	2	1	Integer division operation.

0x51	MLOAD	3	verylow	1	1	Load word from memory.
0x52	MSTORE	3	verylow	2	0	Save word to memory
0x53	MSTORE8	3	verylow	2	0	Save byte to memory.
0x54	SLOAD	200		1	1	Load word from storage
0x55	SSTORE	((value != 0) && (storage_location == 0)) ? 20000 : 5000		1	1	Save word to storage.

COÛT D'UNE TRANSACTION

- Coût total d'une transaction = *GAS_price * GAS_used*
- Priorité aux transactions avec un *GAS_price* élevé.
- Plus l'utilisateur est prêt à payer, plus vite la transaction sera traitée.

MyEtherWallet Behind-The-Scenes



Std Cost for Transfer	Gas Price Std (Gwei)	SafeLow Cost for Transfer	Gas Price SafeLow (Gwei)	Median Wait (s)	Median Wait (blocks)
$0.015	3.5	$0.011	2.6	30	2

Gas-Time-Price Estimator: For transactions sent at block: 6599460

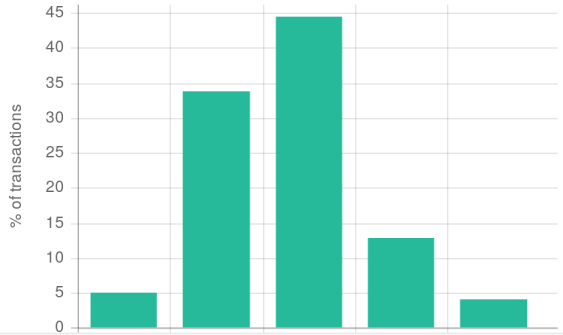
Adjust confirmation time

Avg Time (min)	24.74	Gas Used*	21000
95% Time (min)	61.85	Avg Time (blocks)	98.210721006
Gas Price (Gwei)*	3.5	95% Time (blocks)	245.526802515
Tx Fee (Fiat)	$0.015	Tx Fee (ETH)	0.00007

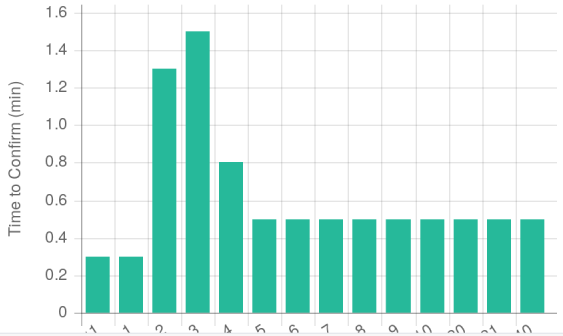
Real Time Gas Use: % Block Limit (last 10)

Last Block: 6599460

Transaction Count by Gas Price



Confirmation Time by Gas Price



Recommended Gas Prices

(based on current network conditions)

Speed	Gas Price (gwei)
SafeLow (<30m)	2.6
Standard (<5m)	3.5
Fast (<2m)	16

Note: Estimates not valid when multiple transactions are batched from the same address or for transactions sent to addresses with many (e.g. > 100) pending

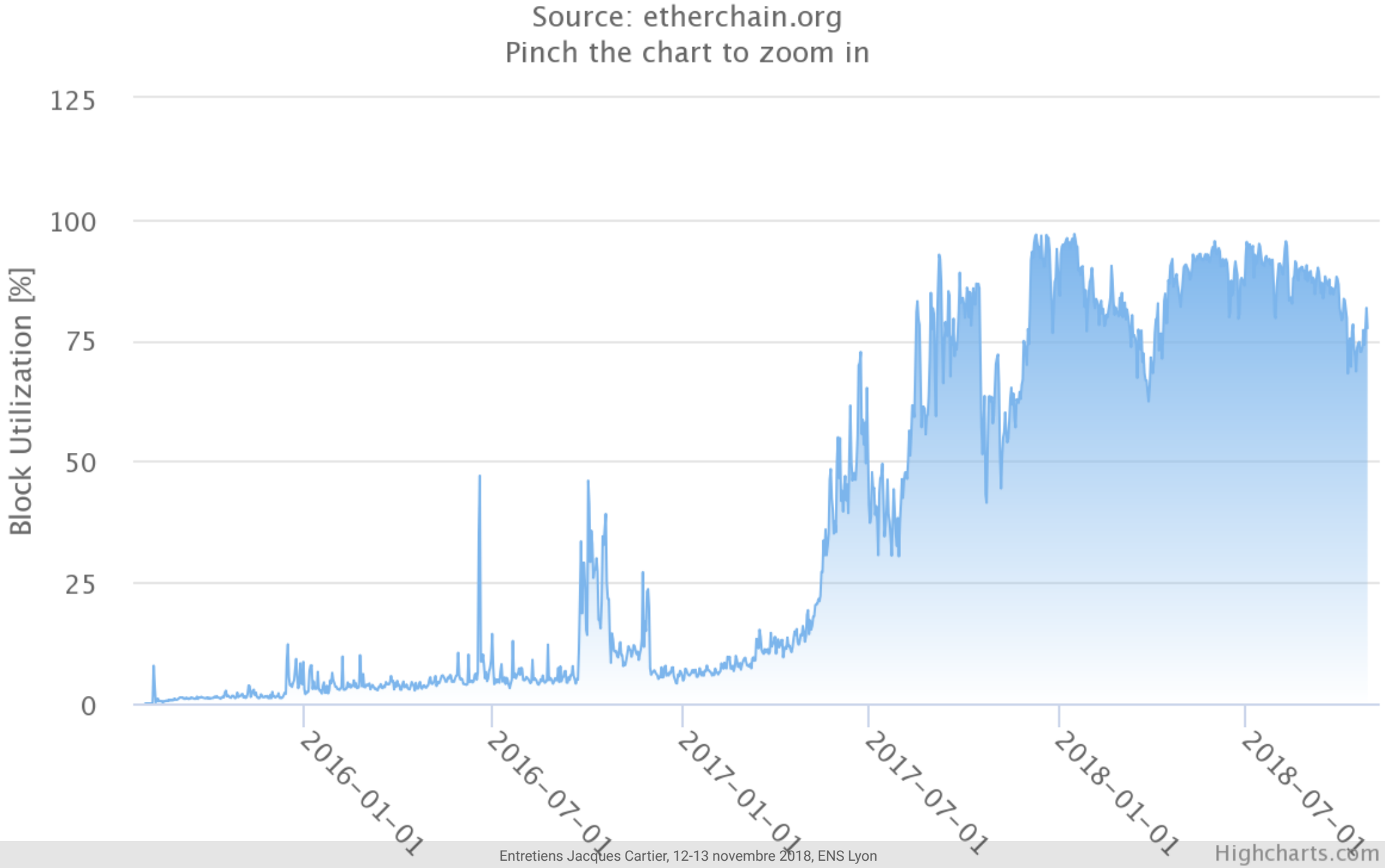
Top 10 Miners by Blocks Mined: Support for user transactions

Miner	Lowest gas price (gwei)	Weighted avg gas price (gwei)	% of total blocks
0xd4383232c8d1dbe0e03bdfab849871fa17e61807	0	13	1
miningpoolhub	1	11	10
Dwarfpool	1	12	2
Ethermine	1	13	27

Misc Stats (Last 1,500 blocks)

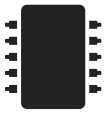
Category	Value
Cheapest Gas Price (gwei)	0
Highest Gas Price (gwei)	14286
Median Gas Price (gwei)	5
Cheapest Transfer Fee	$0.0043

Evolution of the average utilization of Ethereum blocks



PERFORMANCES ACTUELLES

- **block time 15 sec**, 4 blocks/min
- 5959 block/day, 2 174 897 block/year
- **Block Gas limit 8 000 000**
- Daily Gas cap 47 668 965 517
- 76 364 avg gas/tx
- 624 236 tx/day cap
- 433 tx/min
- **7 tx/sec**

EN RÉSUMÉ : POUR LE CALCUL... 

- L'infrastructure Ethereum est un énorme ordinateur Turing complet distribué
- Ultra tolérant aux pannes
- Trés mal exploité car tous les noeuds exécutent les mêmes instructions avec les même données 😐

EN RÉSUMÉ : POUR LE STOCKAGE... 🗄

On est limité par conception à :

- la capacité de stockage des noeuds
- le débit (90 kB / 15 sec => 50 kbits/s)
- le prix du GAS qui fluctue en fonction de l'Ether
- *SSTORE* : 20.000 GAS/Word -> 640.000 GAS/KB
  - 3,5 GWei / GAS -> 0,00224 ETH/KB
  - 200 $/ETH -> 0,448 $/KB

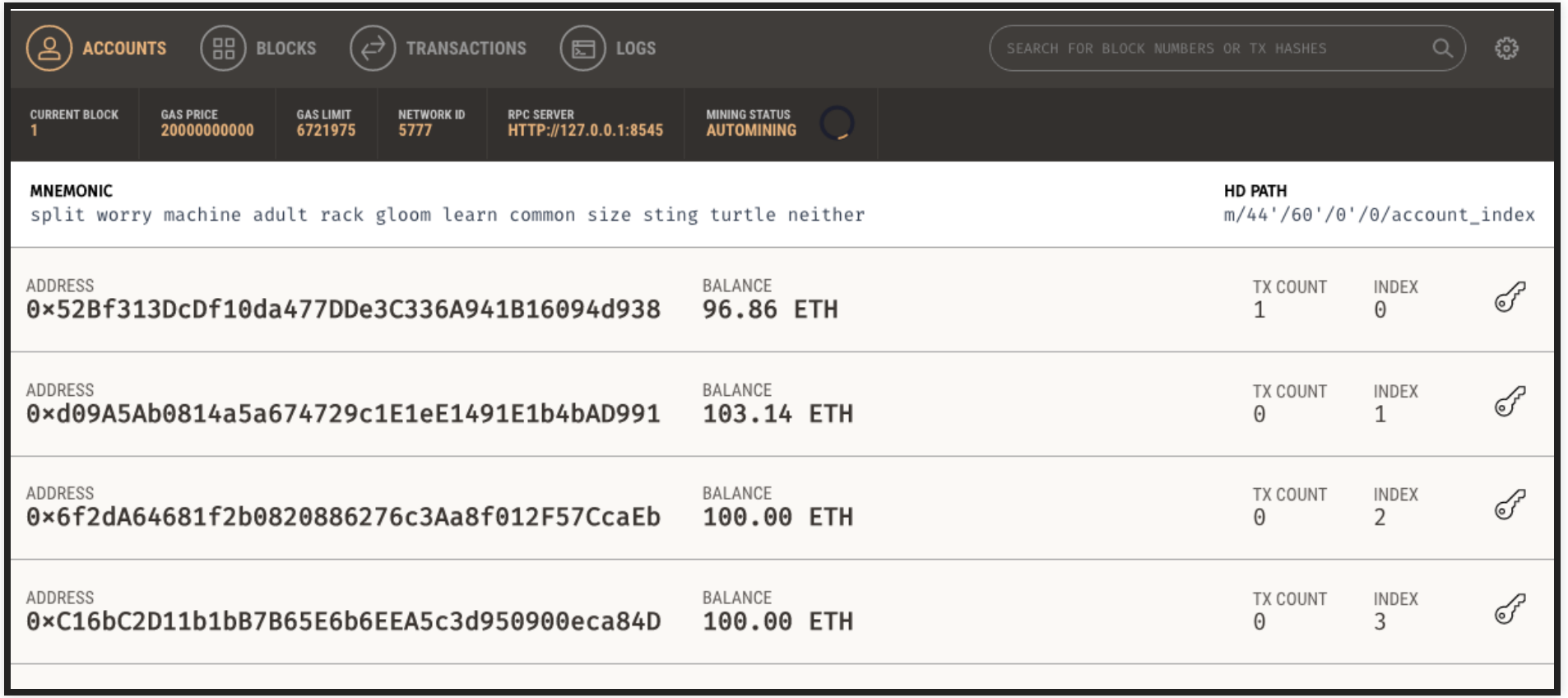
448 000 USD / GBYTES

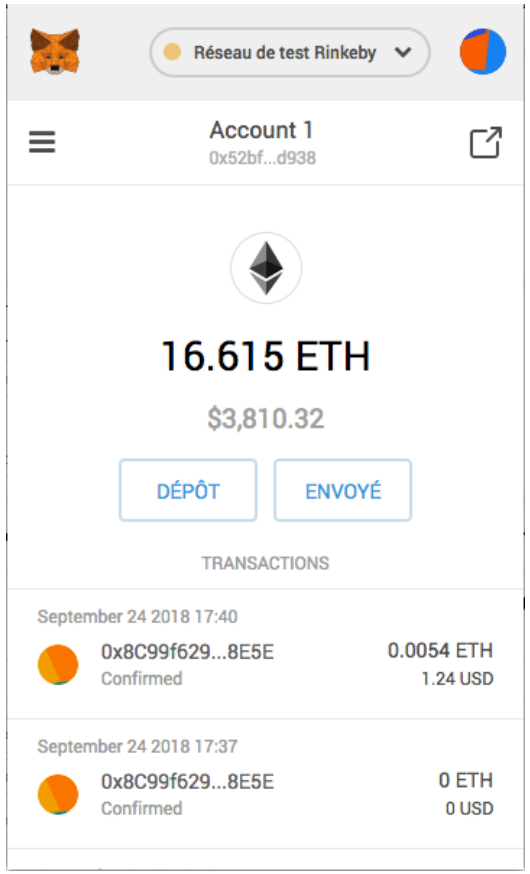
~45 HEURES

(novembre 2018)

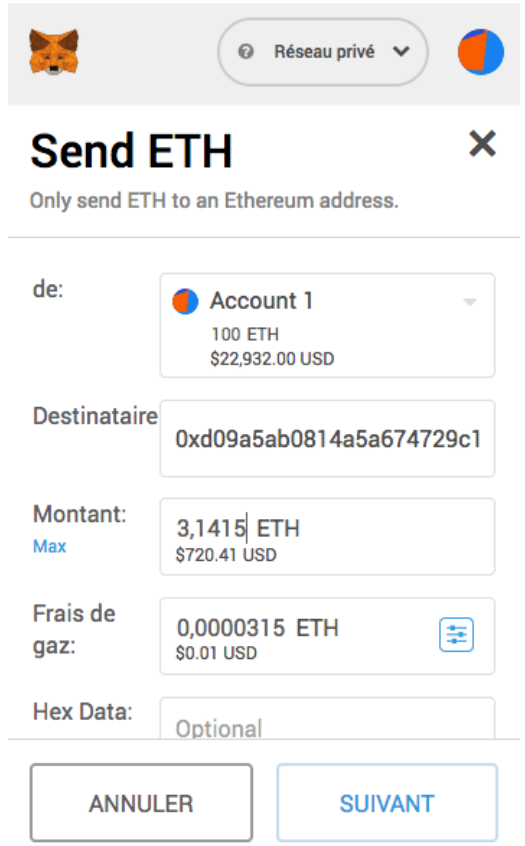
OUTILS DE DÉVELOPPEMENT

GANACHE


ACCOUNTS
BLOCKS
TRANSACTIONS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 1
GAS PRICE 20000000000
GAS LIMIT 6721975
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:8545
MINING STATUS AUTOMINING
MNEMONIC
split worry machine adult rack gloom learn common size sting turtle neither
HD PATH
m/44'/60'/0'/0/account_index
ADDRESS 0×52Bf313DcDf10da477DDe3C336A941B16094d938 BALANCE 96.86 ETH TX COUNT 1 INDEX 0
ADDRESS 0×d09A5Ab0814a5a674729c1E1eE1491E1b4bAD991 BALANCE 103.14 ETH TX COUNT 0 INDEX 1
ADDRESS 0×6f2dA64681f2b0820886276c3Aa8f012F57CcaEb BALANCE 100.00 ETH TX COUNT 0 INDEX 2
ADDRESS 0×C16bC2D11b1bB7B65E6b6EEA5c3d950900eca84D BALANCE 100.00 ETH TX COUNT 0 INDEX 3


Réseau de test Rinkeby
Account 1
0x52bf...d938
16.615 ETH
$3,810.32
DÉPÔT
ENVOYÉ
TRANSACTIONS
September 24 2018 17:40
0x8C99f629...8E5E
Confirmed
0.0054 ETH
1.24 USD
September 24 2018 17:37
0x8C99f629...8E5E
Confirmed
0 ETH
0 USD

METAMASK


Réseau privé
Send ETH
Only send ETH to an Ethereum address.
de:
Account 1
100 ETH
$22,932.00 USD
Destinataire
0xd09a5ab0814a5a674729c1
Montant:
Max
3,1415 ETH
$720.41 USD
Frais de gaz:
0,0000315 ETH
$0.01 USD
Hex Data:
Optional
ANNULER
SUIVANT

TRANSACTION

TX HASH
0×9e2fd9595b4b596c3d798508a5e20c0f8980f95263b1f928ffa3d6ff9ac34e0a

VALUE TRANSFER

FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE
0×52bf313dcdf10da477dde3c336a941b16094d938	0×d09a5ab0814a5a674729c1e1ee1491e1b4bad991	21000	3141500000000000000

TRANSACTION *DÉTAIL*

Transaction 0x512322644a8bb57fe3fe00977ba462daef2da571a9ee267fc74a969973eae7df

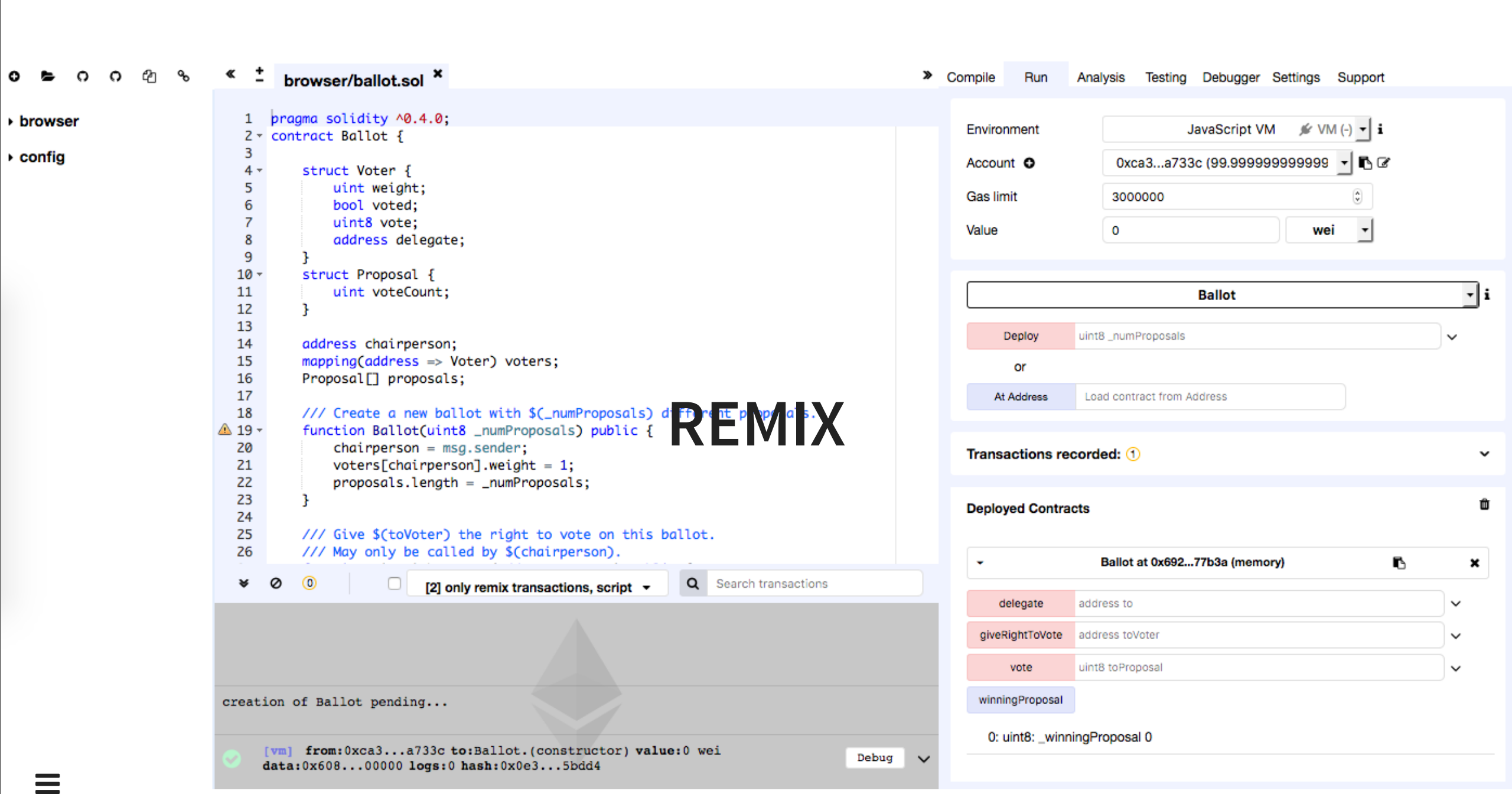
Overview | Comments

Buy | Crypto Loan

Transaction Information

Tools & Utilities

TxHash:	0x512322644a8bb57fe3fe00977ba462daef2da571a9ee267fc74a969973eae7df
TxReceipt Status:	Success
Block Height:	6686011 (1 Block Confirmation)
TimeStamp:	17 secs ago (Nov-11-2018 06:00:36 PM +UTC)
From:	0xc98f4c64c63ce7d10cb7615e0100ffcfc912aba3
To:	0x5d2c3da03b5bc33673b921e8cf5bbae2100e7dc0
Value:	0.054343840721857432 Ether ($11.37)
Gas Limit:	21000
Gas Used By Transaction:	21000 (100%)
Gas Price:	0.000000001401000001 Ether (1.401000001 Gwei)
Actual Tx Cost/Fee:	0.00002942100002 Ether ($0.006158)
Nonce & {Position}:	1 | {123}


browser
config
browser/ballot.sol
Compile
Run
Analysis
Testing
Debugger
Settings
Support
pragma solidity ^0.4.0;
contract Ballot {
struct Voter {
uint weight;
bool voted;
uint8 vote;
address delegate;
}
struct Proposal {
uint voteCount;
}
address chairperson;
mapping(address => Voter) voters;
Proposal[] proposals;
/// Create a new ballot with $(_numProposals) different proposals.
function Ballot(uint8 _numProposals) public {
chairperson = msg.sender;
voters[chairperson].weight = 1;
proposals.length = _numProposals;
}
/// Give $(toVoter) the right to vote on this ballot.
/// May only be called by $(chairperson).
REMIX
[2] only remix transactions, script
Search transactions
creation of Ballot pending...
[vm] from:0xca3...a733c to:Ballot.(constructor) value:0 wei
data:0x608...00000 logs:0 hash:0x0e3...5bdd4
Debug
Environment
JavaScript VM
VM (-)
Account
0xca3...a733c (99.999999999999
Gas limit
3000000
Value
0
wei
Ballot
Deploy
uint8 _numProposals
or
At Address
Load contract from Address
Transactions recorded:
Deployed Contracts
Ballot at 0x692...77b3a (memory)
delegate
address to
giveRightToVote
address toVoter
vote
uint8 toProposal
winningProposal
0: uint8: _winningProposal 0

CONCLUSION

- Miner de l'ether = Sécuriser le réseau = Vérifier les traitements
- Par conception la blockchain Ethereum garantie :
  - l'immutabilité des données,
  - l'exécution et l'accès sans censure possible.
- Analyser un Smart Contract en terme de consommation de GAS pour maitriser le coût operationnel.
- Maximiser les calculs et le stockage *offchain*.

⁇ QUESTIONS ⁇

Cette présentation est disponible sur
https://gitpitch.com/jpgelas/EJC

:wq!

LIENS UTILES

- https://hackernoon.com/ether-purchase-power-df40a38c5a2f
- OPCODE list + GAS : https://docs.google.com/spreadsheets/d/1m89CVujrQe5LAFJ8-YAUCcNK950dUzMQPMJBxRtGCqs/edit#gid=0
- Ethernodes (28/10/2018 -> 13320 nodes) : https://www.ethernodes.org/network/1
- https://www.etherchain.org/charts/averageBlockUtilization
- https://etherscan.io/
- https://medium.com/coinmonks/storing-on-ethereum-analyzing-the-costs-922d41d6b316