Web3, NFT
au-delà du bullshit

Les blockchains en pratique

Par Samuel Liard

Mars 2022

Disclaimer !

Je ne suis pas un spécialiste des blockchains

Cette présentation retrace ma veille sur le sujet

Fonction de hachage cryptographique

- Fonction à sens unique, non bijective
- Calcul très simple
- Déterministe
- Effet avalanche
- Bonne résistance aux collisions

Attaque des anniversaires

n : nombre d’éléments
m : nombre de hash possible
p(n) : probabilité d’avoir une collision

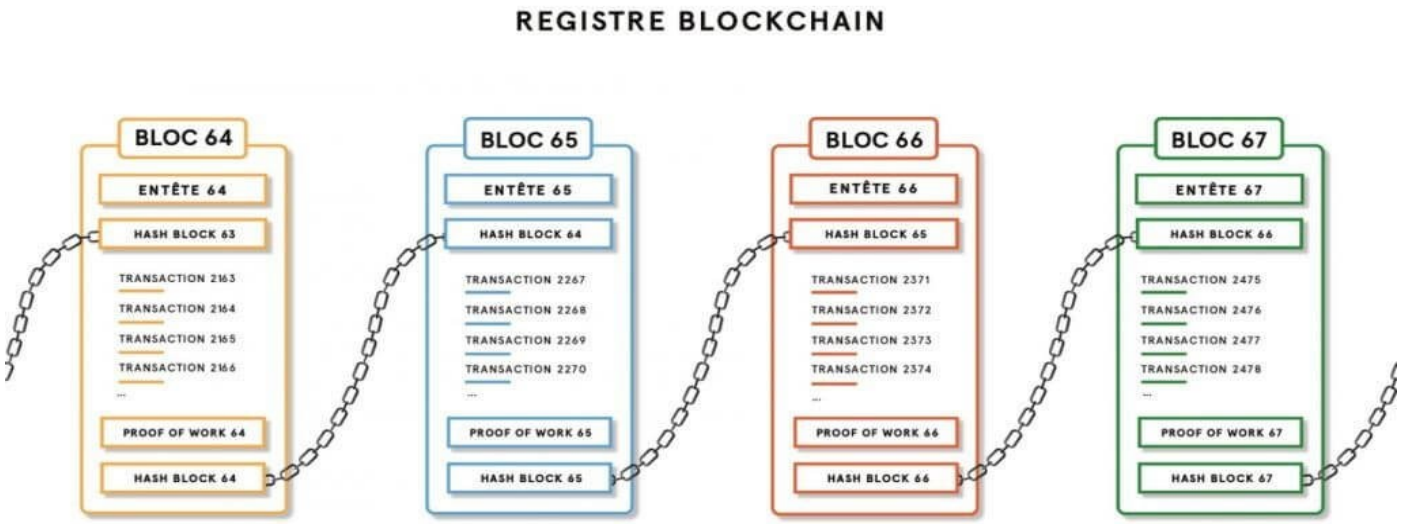
$$p(n) \approx \frac{n^2}{2m}, \qquad n \approx \sqrt{2m \times p(n)}$$

Avec un hash sur 16 bits, le 37ième généré à 1% de change de déjà exister
Après 430 hash, il y a 75% d’avoir des collisions.

Avec un hash sur 256 bits, il faut plus de 1,5 × 10^37 éléments pour arriver à une probabilité de collision de 0,1%

Gagner au loto c’est 1 chance sur 19 068 840.

Une blockchain



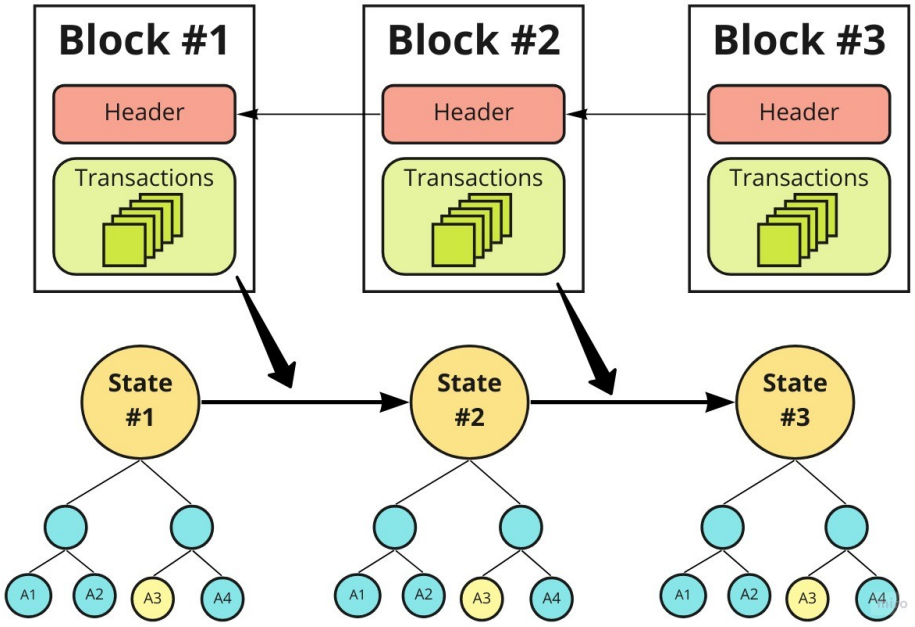
Concensus

ArchEthic ARCH Consensus

Delegated Proof of Stake

Proof of Importance

Blockchain state



Smart Contract

- Programmes irrévocables
- Jeu d’instructions limité
- Transparent
- State transition function = fonction déterministe

https://github.com/crytic/evm-opcodes

Opcode	Name	Description	Extra Info	Gas
0x00	STOP	Halts execution	-	0
0x01	ADD	Addition operation	-	3
0x02	MUL	Multiplication operation	-	5
0x03	SUB	Subtraction operation	-	3
0x04	DIV	Integer division operation	-	5
0x05	SDIV	Signed integer division operation (truncated)	-	5
0x06	MOD	Modulo remainder operation	-	5
0x07	SMOD	Signed modulo remainder operation	-	5
0x08	ADDMOD	Modulo addition operation	-	8
0x09	MULMOD	Modulo multiplication operation	-	8
0x0a	EXP	Exponential operation	-	10*

```solidity
pragma solidity ≥0.8.4;

contract ForLoop {
    function plusplusi(uint256 _number) external pure {
        unchecked {
            for (uint256 i; i < _number; ++i) {
                uint256 j = i;
            }
        }
    }

    function iplusplus(uint256 _number) external pure {
        unchecked {
            for (uint256 i; i < _number; i++) {
                uint256 j = i;
            }
        }
    }
}
```

```
[PASS] testGas_iplusplus_0() (gas: 1452)
[PASS] testGas_plusplusi_0() (gas: 1497)
-45

[PASS] testGas_iplusplus_1() (gas: 1508)
[PASS] testGas_plusplusi_1() (gas: 1569)
-61

[PASS] testGas_iplusplus_10() (gas: 2078)
[PASS] testGas_plusplusi_10() (gas: 2029)
49

[PASS] testGas_iplusplus_100() (gas: 7053)
[PASS] testGas_plusplusi_100() (gas: 6597)
456

[PASS] testGas_iplusplus_1000() (gas: 57519)
[PASS] testGas_plusplusi_1000() (gas: 52452)
5067

[PASS] testGas_iplusplus_10000() (gas: 561519)
[PASS] testGas_plusplusi_10000() (gas: 511474)
50045
```

Smart Contract

- Vyper, proche de python
- Solidity, proche de Java

- Outils Truffle


```solidity
pragma solidity >=0.5.0 <0.7.0;

contract Coin {
    // The keyword "public" makes variables
    // accessible from other contracts
    address public minter;
    mapping (address => uint) public balances;
    mapping (address => mapping (address => uint256)) public allowed;

    // Events allow clients to react to specific
    // contract changes you declare
    event Transfer (address from, address to, uint amount);
    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
    event MintingRightTransferred(address indexed oldMinter, address indexed newMinter);

    string public symbol = "WIKI";
    string public name = "WikiArticleToken";
    uint256 public totalSupply;

    // Constructor code is only run when the contract
    // is created
    constructor() public {
        minter = msg.sender;
    }

    // Sends an amount of newly created coins to an address
    // Can only be called by the contract creator
    function mint(address receiver, uint amount) public {
        require(msg.sender == minter);
        require(amount <= 2**256-1); // be aware of high amounts since overflow exist
        balances[receiver] += amount;
        totalSupply += amount;
        emit Transfer(address(0), receiver, amount);
    }
```

Smart Contract

- https://hardhat.org/
- https://eth-brownie.readthedocs.io/en/stable/ → python
- https://dapp.tools/
- https://remix.ethereum.org/
- Foundry Ethereum development toolbox → Rust

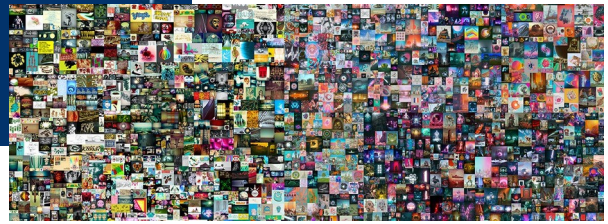
- Web3js/Ethersjs
- Moralis
- UseDapp
- https://github.com/scaffold-eth/scaffold-eth

Le web3

Web3 is the stack of protocols that enable fully decentralized applications.

- Decentralized web infrastructure
- Ownership (of data, content, and platform)
- Native digital payments
- Self-sovereign identity
- Distributed, trust-less, & robust infrastructure
- Open, public, composable back ends

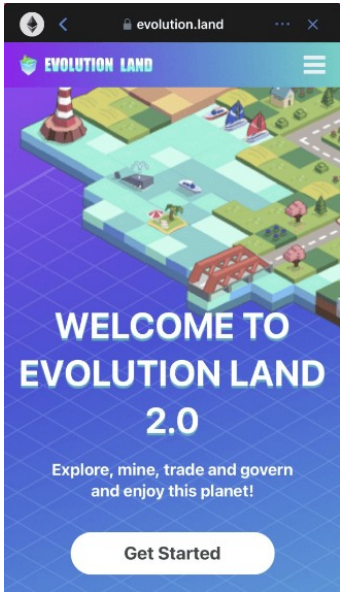
NFT



Jeux à base de NFT

Sorare

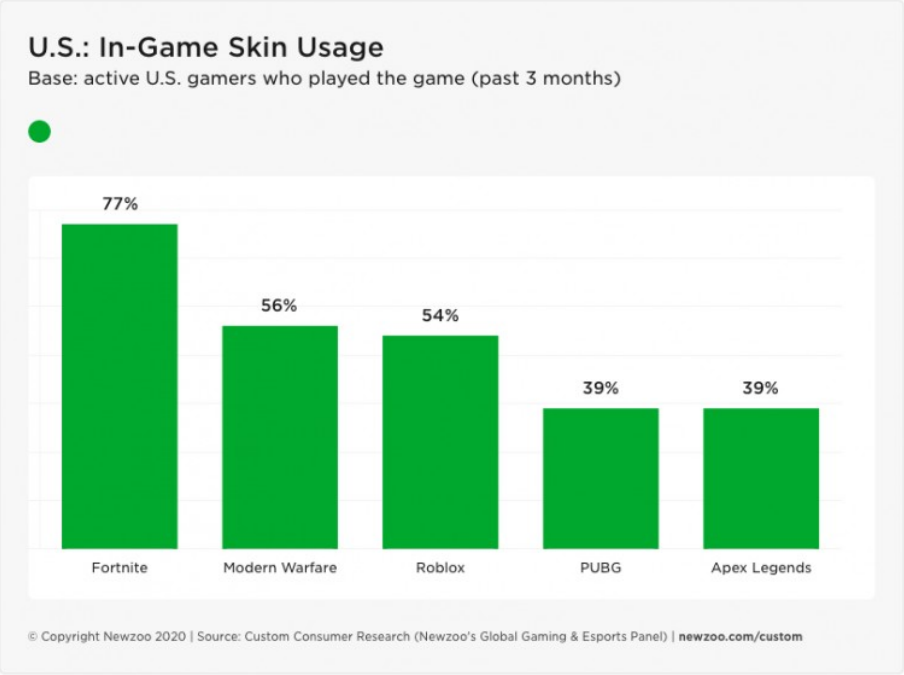
CryptoKitties



Evolution Land

Marché

- Fornite : Près de 80 % de ses joueurs récents s'engagent d'une manière ou d'une autre
- Le jeu vidéo sur smartphone a rapporté 82 milliards d’euros en 2021
  - PUBG Mobile : 2,8 milliards $
  - Honor of Kings : 2,8 milliards $
  - Genshin Impact : 1,8 milliards $



NFT

- Token ERC-20 → Fongible

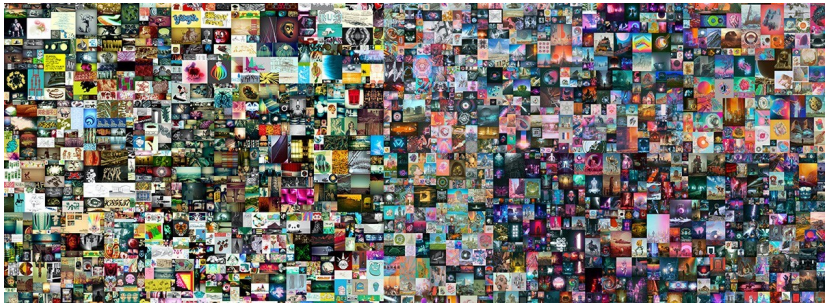
```
function name() public view returns (string)
function symbol() public view returns (string)
function decimals() public view returns (uint8)
function totalSupply() public view returns (uint256)
function balanceOf(address _owner) public view returns (uint256 balance)
function transfer(address _to, uint256 _value) public returns (bool success)
function transferFrom(address _from, address _to, uint256 _value) public returns (bool success)
function approve(address _spender, uint256 _value) public returns (bool success)
function allowance(address _owner, address _spender) public view returns (uint256 remaining)
```

- Token ERC-721 → Non fongible

```
function balanceOf(address _owner) external view returns (uint256);
function ownerOf(uint256 _tokenId) external view returns (address);
function safeTransferFrom(address _from, address _to, uint256 _tokenId, bytes data) external payable;
function safeTransferFrom(address _from, address _to, uint256 _tokenId) external payable;
function transferFrom(address _from, address _to, uint256 _tokenId) external payable;
function approve(address _approved, uint256 _tokenId) external payable;
function setApprovalForAll(address _operator, bool _approved) external;
function getApproved(uint256 _tokenId) external view returns (address);
function isApprovedForAll(address _owner, address _operator) external view returns (bool);
```

- Token ERC-1155
  - transferSingle, transferBatch, URI

NFT



69 millions de $

Beeple (b. 1981)
EVERYDAYS: THE FIRST 5000 DAYS
token ID: 40913
wallet address:
0xc6b0562605D35eE710138402B878ffe6F2E23807
smart contract address:
0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756
non-fungible token (jpg)
21,069 x 21,069 pixels (319,168,313 bytes)
Minted on 16 February 2021. This work is unique.

23. tokenURI

_tokenId (uint256)

40913

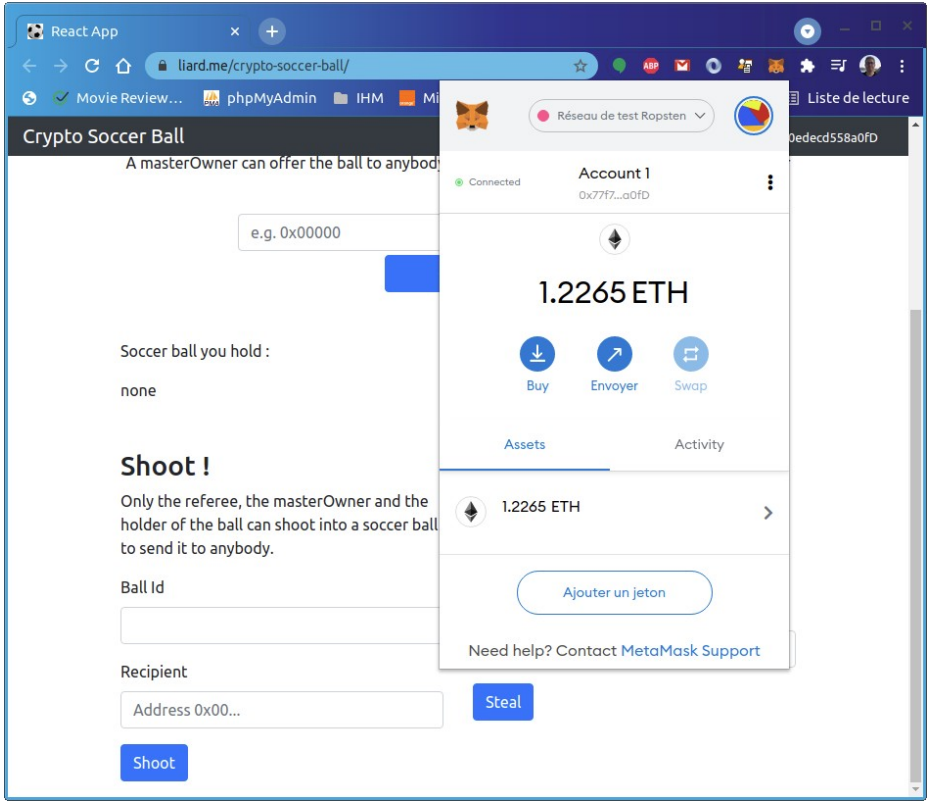
Query

string

[**tokenURI(uint256)** method Response]

» *string* : ipfs://ipfs/QmPAg1mjxcEQPPtqsLoEcauVedaeMH81WXDPvPx3VC5zUz

Jeux à base de NFT



Nat Eliason
@nateliason

Alright, so, time for a VERY painful story about how in my excitement about learning solidity yesterday I made a mistake that let someone steal $30,000 from me.

💪💪💪

Traduire le Tweet

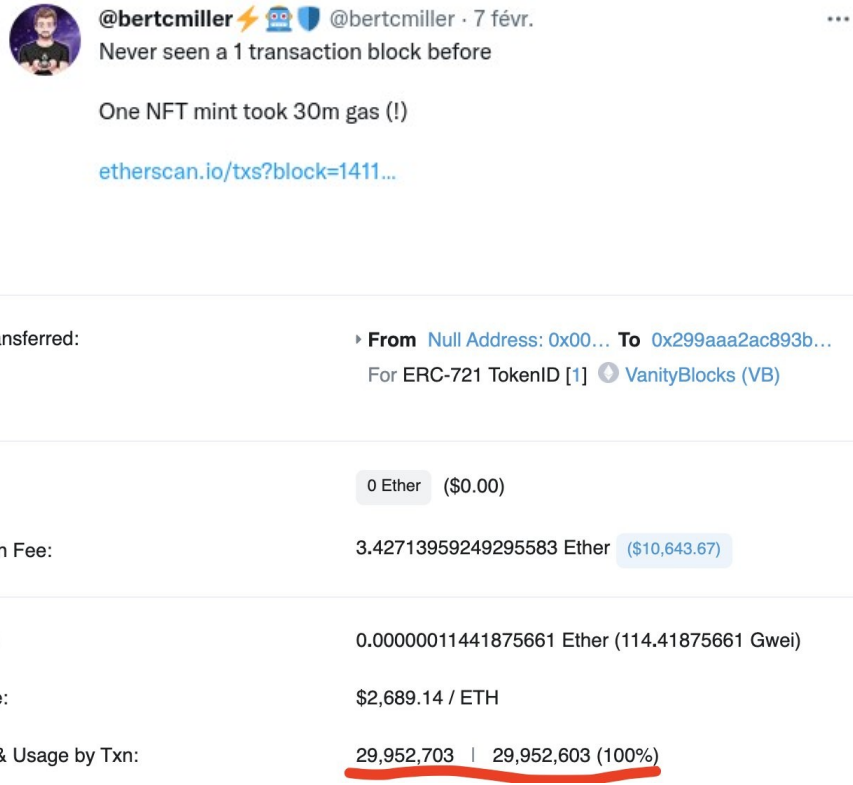
> **Nat Eliason** @nateliason · 10 mai
> Deployed my first "hello world" style contract on the test network this morning 😄
> .
>
> This is the most fun I've had learning something in a long time

1:58 PM · 11 mai 2021 · Twitter Web App

NFT

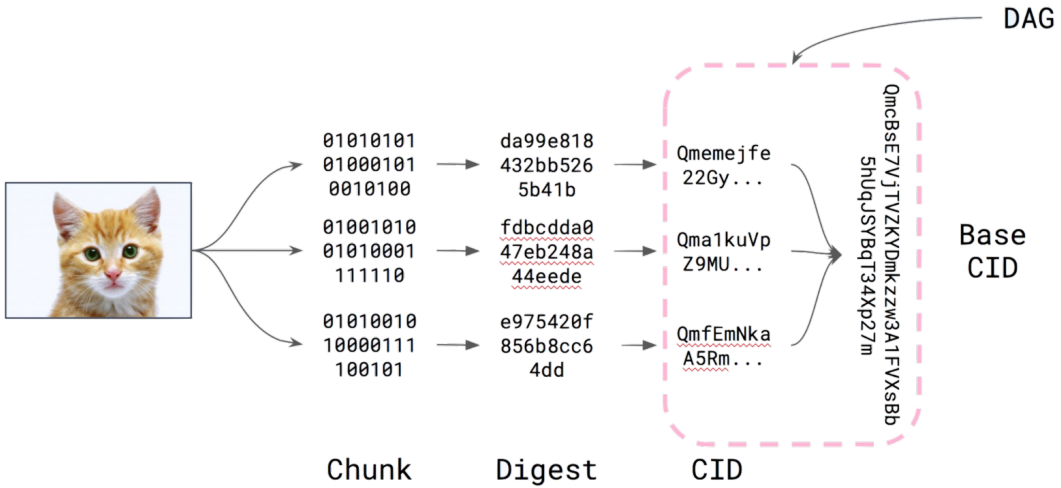
```
Replacing 'Photo'
-----------------
> transaction hash:    0xd87e545c6c234360967d8b945ab907c2c932efa344e8dd4181f82054a7603890
> Blocks: 0            Seconds: 0
> contract address:    0x6d996E0bC5d6D2c626fbc2ceD48ed9221Eb69f70
> block number:        95
> block timestamp:     1643619920
> account:             0x2F1bc1A46a5643a8827554F29C5499291E9d2663
> balance:             93.3453385
> gas used:            3528674 (0x35d7e2)
> gas price:           20 gwei
> value sent:          0 ETH
> total cost:          0.07057348 ETH


> Saving migration to chain.
> Saving artifacts
-------------------------------------
> Total cost:          0.07057348 ETH
```


@bertcmiller @bertcmiller · 7 févr.
Never seen a 1 transaction block before
One NFT mint took 30m gas (!)
etherscan.io/txs?block=1411...
Tokens Transferred:
From Null Address: 0x00... To 0x299aaa2ac893b...
For ERC-721 TokenID [1] VanityBlocks (VB)
Value:
0 Ether ($0.00)
Transaction Fee:
3.42713959249295583 Ether ($10,643.67)
Gas Price:
0.000000011441875661 Ether (114.41875661 Gwei)
Ether Price:
$2,689.14 / ETH
Gas Limit & Usage by Txn:
29,952,703 | 29,952,603 (100%)

InterPlanetary File System

- Réseau P2P
- Adréssé par le contenu
- IPNS (Inter-Planetary Naming System)



InterPlanetary File System

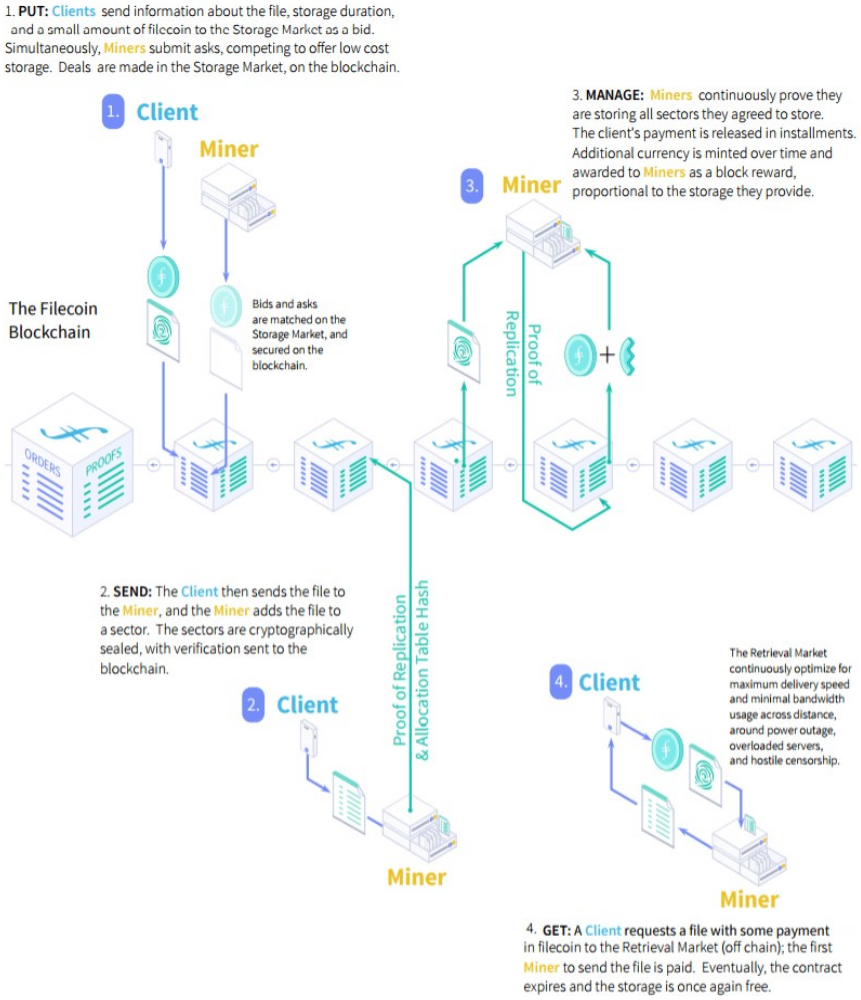

```
{
   title: "EVERYDAYS: THE FIRST 5000 DAYS",
   name: "EVERYDAYS: THE FIRST 5000 DAYS",
   type: "object",
   imageUrl: "https://ipfsgateway.makersplace.com/ipfs/QmZ15eQX8FPjfrtdX3QYbrhZxJpbLpvDpsgb2p3VEH8Bqq",
   description: "I made a picture from start to finish every single day from May 1st, 2007 - January 7th, 2021. This is every motherfucking one of those pictures.",
 - attributes: [
     - {
           trait_type: "Creator",
           value: "beeple"
       }
   ],
 - properties: {
     - name: {
           type: "string",
           description: "EVERYDAYS: THE FIRST 5000 DAYS"
       },
     - description: {
           type: "string",
           description: "I made a picture from start to finish every single day from May 1st, 2007 - January 7th, 2021. This is every motherfucking one of those pictures."
       },
     - preview_media_file: {
           type: "string",
           description: "https://ipfsgateway.makersplace.com/ipfs/QmZ15eQX8FPjfrtdX3QYbrhZxJpbLpvDpsgb2p3VEH8Bqq"
       },
     - preview_media_file_type: {
           type: "string",
           description: "jpg"
       },
     - created_at: {
           type: "datetime",
           description: "2021-02-16T00:07:31.674688+00:00"
       },
     - total_supply: {
           type: "int",
           description: 1
       },
     - digital_media_signature_type: {
           type: "string",
           description: "SHA-256"
       },
     - digital_media_signature: {
           type: "string",
           description: "6314b55cc6ff34f67a18e1ccc977234b803f7a5497b94f1f994ac9d1b896a017"
       },
     - raw_media_file: {
           type: "string",
           description: "https://ipfsgateway.makersplace.com/ipfs/QmXkxpwAHCtDXbbZHUwqtFucG1RMS6T87vi1CdvadfL7qA"
       }
   }
}
```

LibP2P

- Projet open source
- Gère :
  - Transport (tcp, udp, websocket…)
  - Stream muxers
  - Gestion de connexion
  - Peer routing / discovery

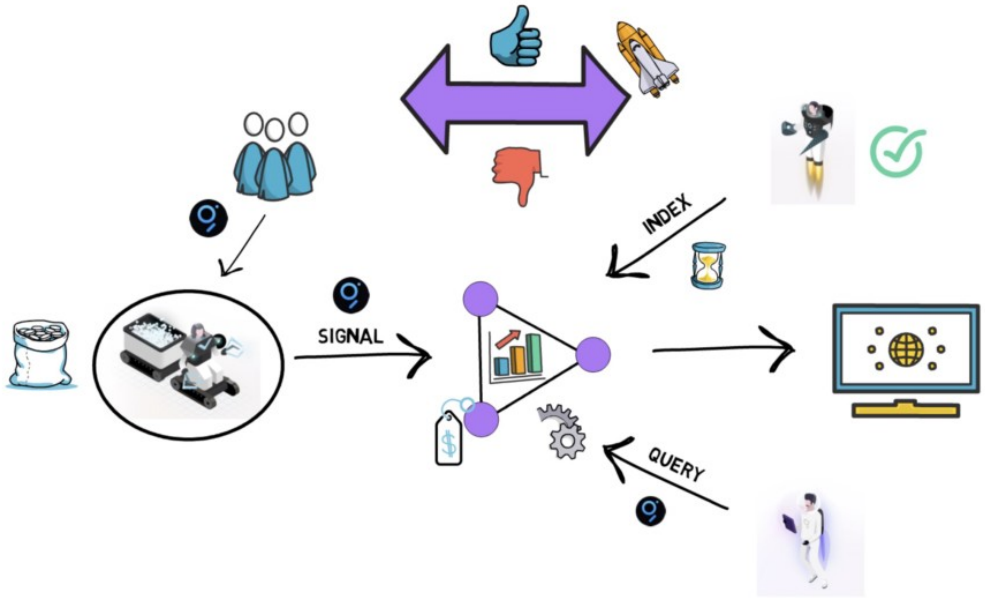
FileCoin

- Espace de stockage
- Place de marché



The Graph

- Google Of Blockchains
- Utilise GraphQL



UNIRIS

My body as a private key

New Blockchain Generation

Sustainable, Scalable, Secure and Inclusive

Earth-friendly

3.6 Billion times less energy consumption, by using the ARCH (Atomic Rotating Commitment Heuristic) consensus based on heuristic miners' election and a polymorphic worldwide replication. Each Uniris transaction only needs 0.42w of energy (0.1g of sugar).

Smart-er Contracts

In addition to running the blockchain itself, Uniris smart contracts provide the community On-Chain governance. Uniris smart-contracts are natively triggerable, upgradable, formal and easy to program helping in development of reliable applications.

Aviation Safety

Beyond just PoW (51%) or dBFT (66%), the Uniris blockchain provides a collaborative & Formal Proof-of-Work allowing to handle 90% of malicious miners, ushering an inclusive and new age of decentralized security based on the standards of aviation safety (fraud risk $< 10^{-9}$).

Super Fast & Limitless

Without impacting the global validation, the heuristic polymorphic replication provides a linear increase of the capacity (in storage and number of validations) allowing to reach million transaction validations per second ... no magic just read the Yellow Paper.