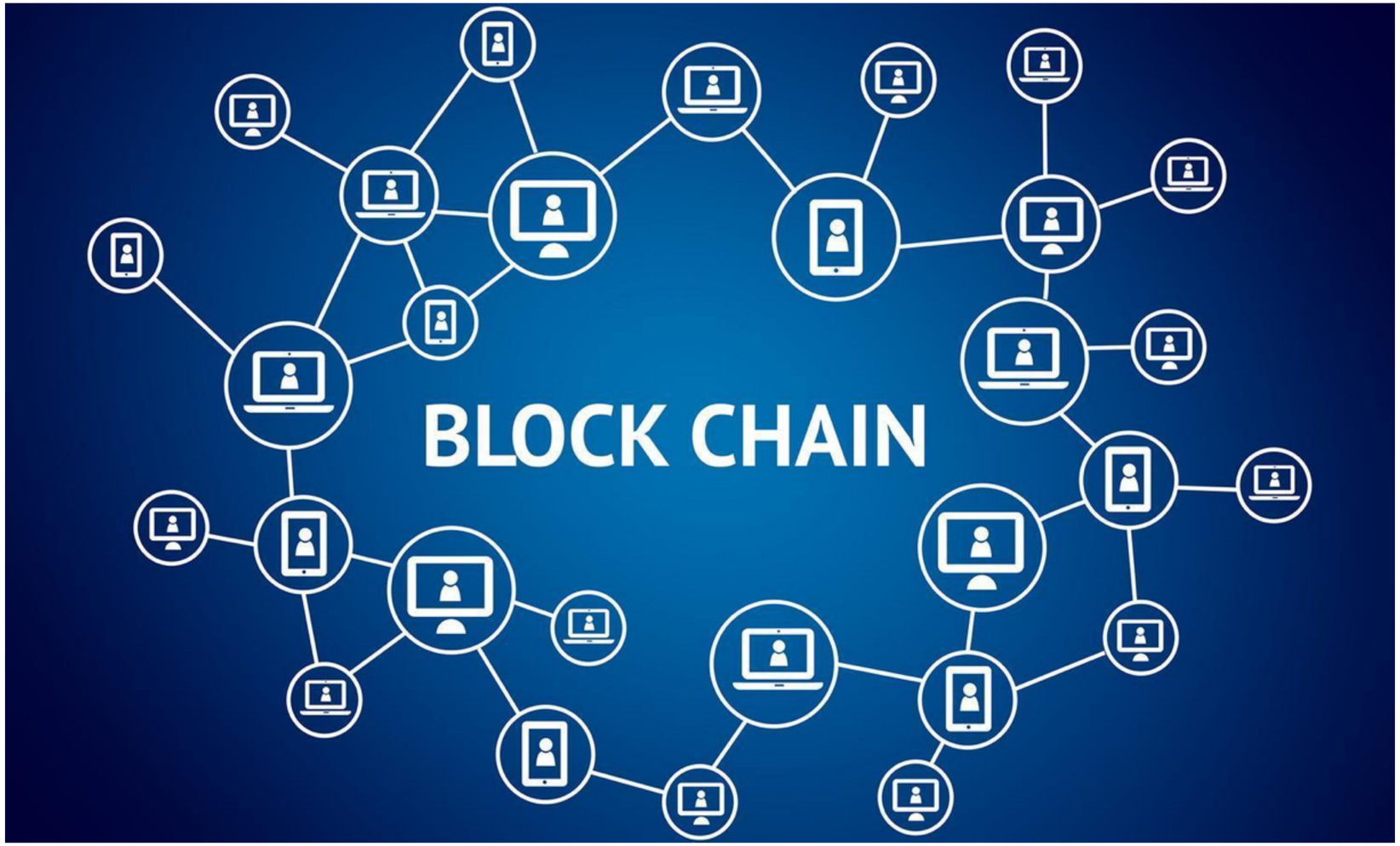


Post-internet Revolution

IT Talk BP2S - May 2017 - Vincent Jugé

What is it ?

« Blockchain is a peer-to-peer trust-less system, immutable and censorship resistant »

-K. Loaec

Ok .....?

Origins : Bitcoin

2008/09

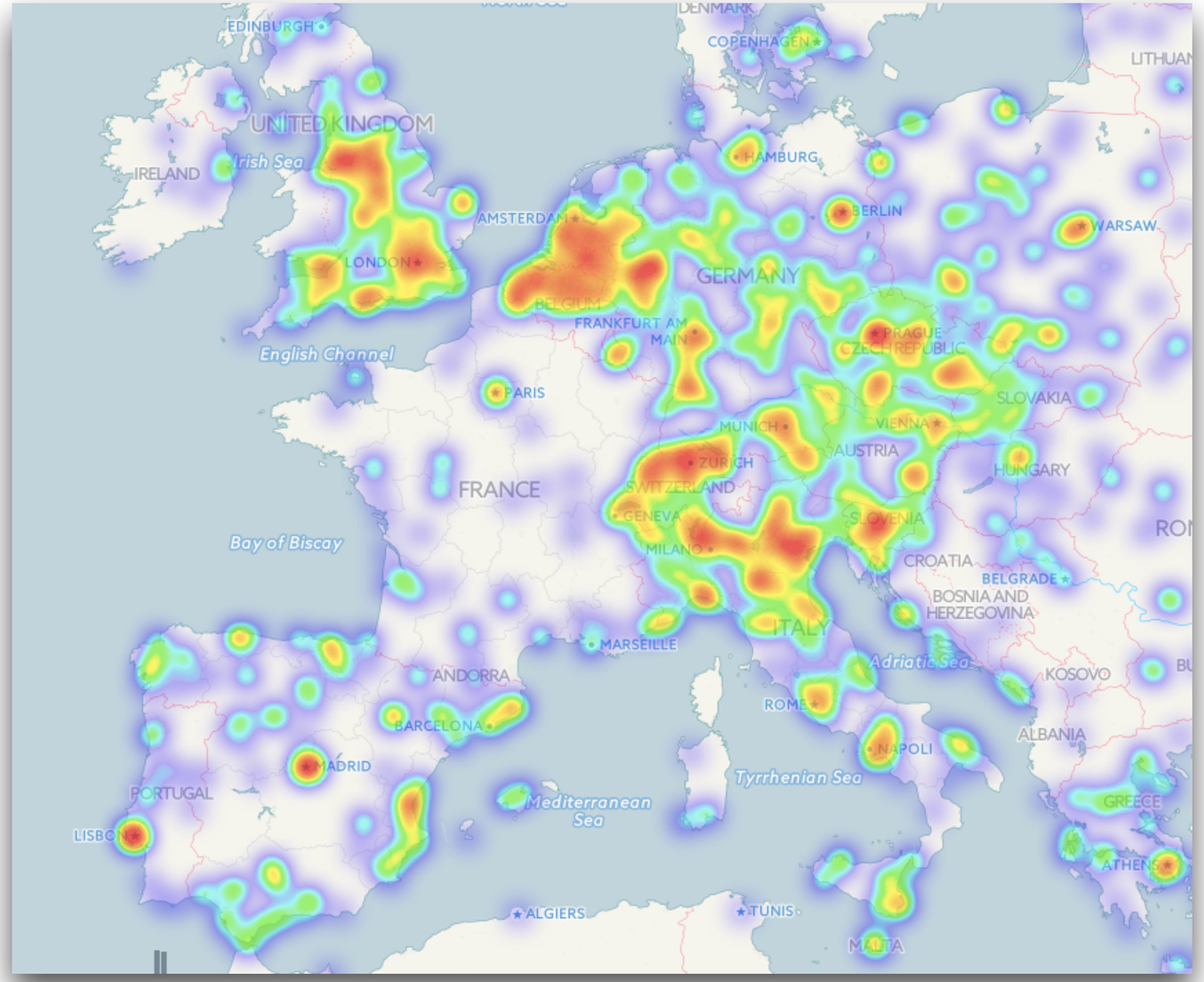
Crypto-currency

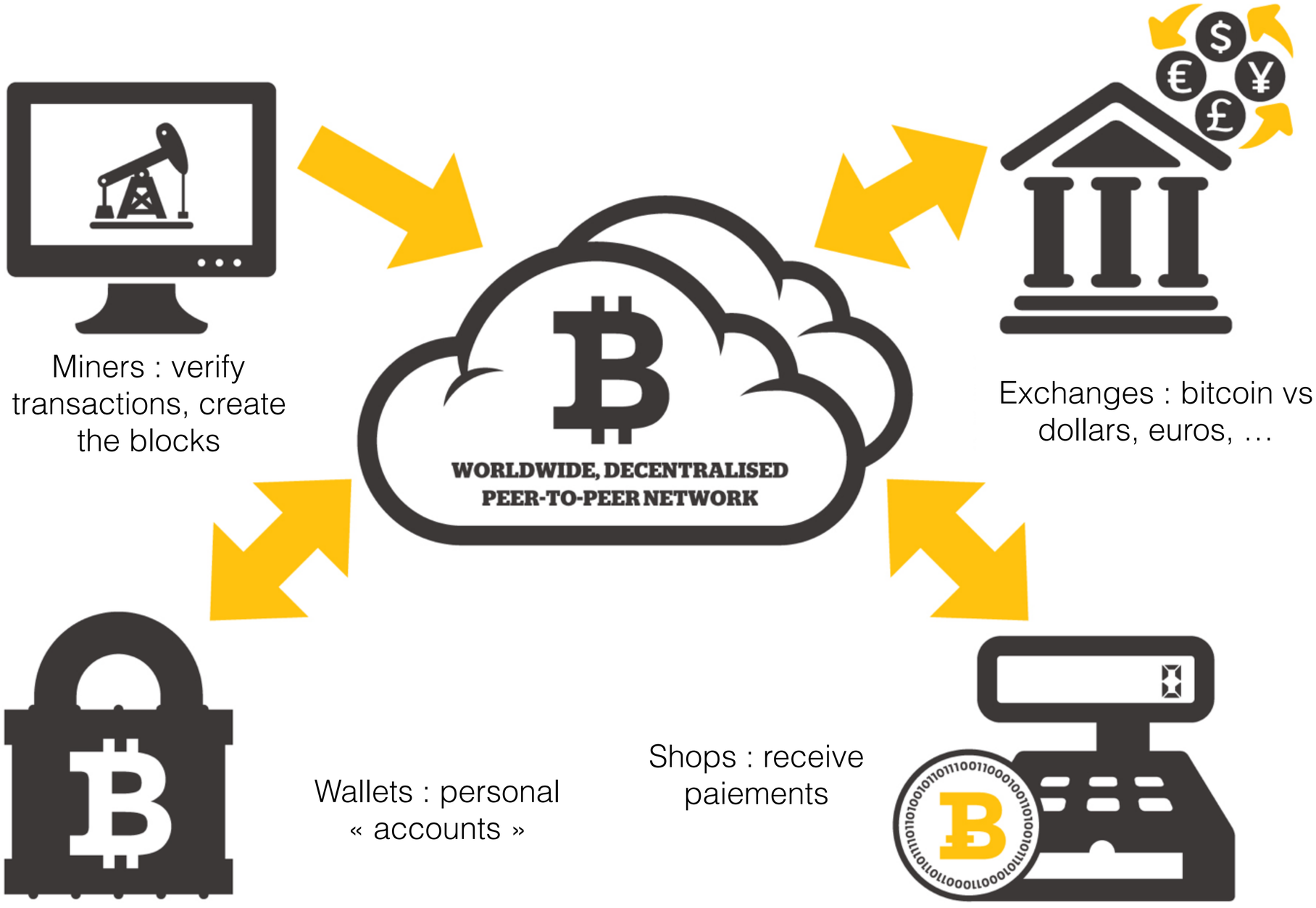
Introduces « Blockchain » technology


bitcoin
bitcoin
ACCEPTED HERE


bitcoinATM

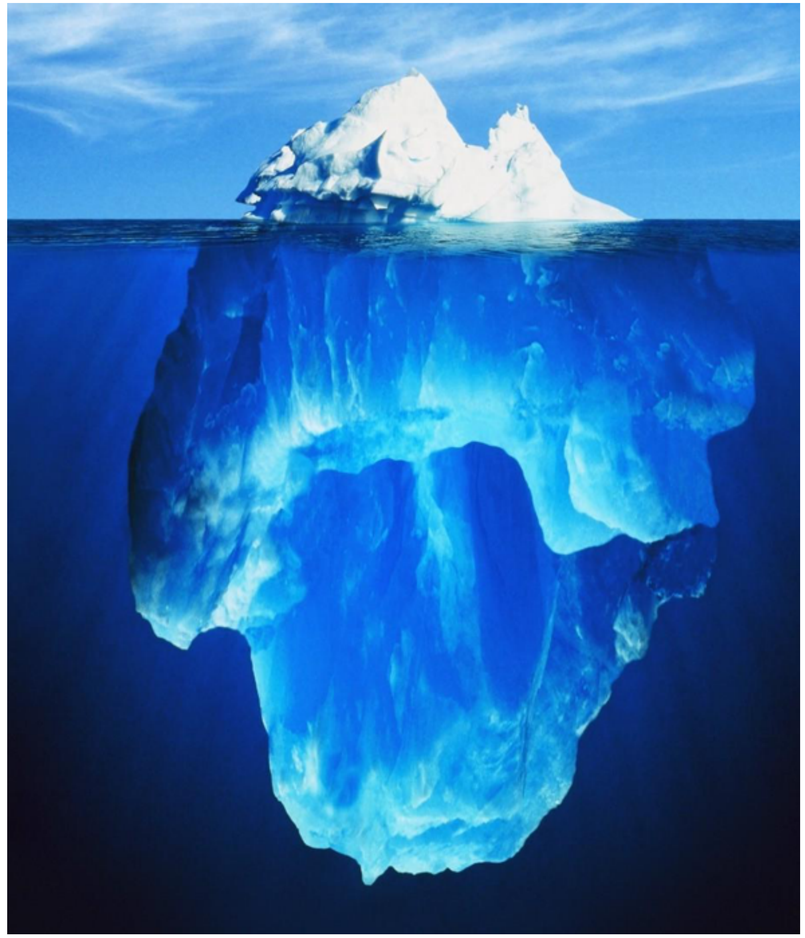

Invoice Status
Circle Interactive
67de52db0b3edd891e53a1
0.0001 BTC
Pay with Bitcoin
13:48
0.0001 BTC = 0.02 GBP
English | Support | Powered by BitPay.


EDINBURGH
COPENHAGEN
UNITED KINGDOM
IRELAND
Irish Sea
HAMBURG
AMSTERDAM
BERLIN
WARSAW
LONDON
GERMANY
BELGIUM
FRANKFURT AM MAIN
PRAGUE
CZECH REPUBLIC
English Channel
PARIS
SLOVAKIA
MUNICH
VIENNA
AUSTRIA
ZURICH
HUNGARY
FRANCE
SWITZERLAND
GENEVA
SLOVENIA
Bay of Biscay
MILANO
CROATIA
BELGRADE
BOSNIA AND HERZEGOVINA
ITALY
MARSEILLE
Adriatic Sea
KOSOVO
ANDORRA
ROME
BARCELONA
ALBANIA
NAPOLI
MADRID
Tyrrhenian Sea
PORTUGAL
Mediterranean Sea
GREECE
LISBON
ATHENS
ALGIERS
TUNIS
MALTA


Miners : verify transactions, create the blocks
WORLDWIDE, DECENTRALISED PEER-TO-PEER NETWORK
Exchanges : bitcoin vs dollars, euros, …
Wallets : personal « accounts »
Shops : receive paiements

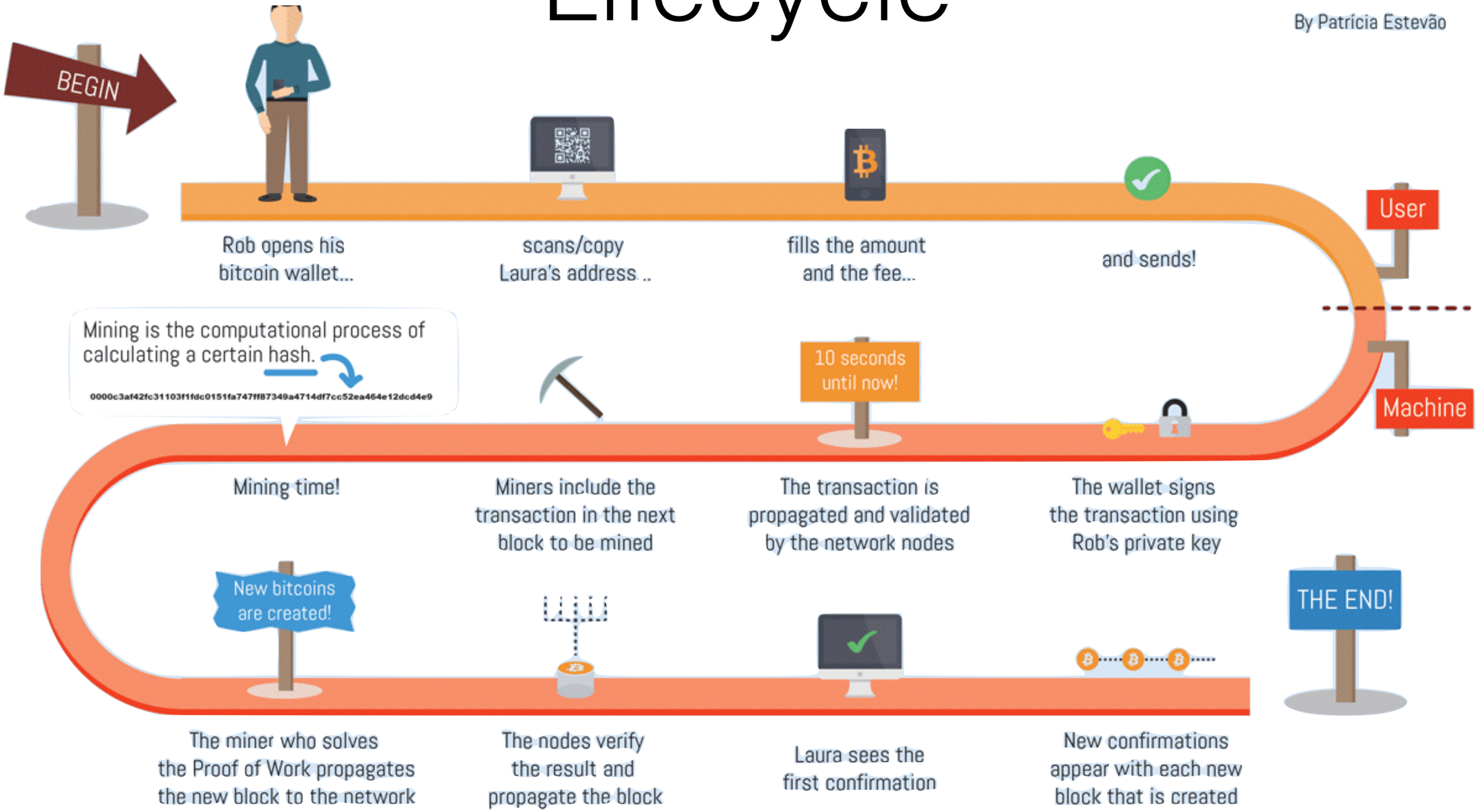

AT&T 4G
12:25 PM
Wallet Home
0.30519173 BTC
Send Money
My Transactions
Receive Money
Total Transactions
4
Total Received
0.50519173 BTC
Total Sent
0.20 BTC
Final Balance
0.30519173 BTC
This Is Your Bitcoin Address

How does it works ?



Lifecycle

By Patrícia Estevão

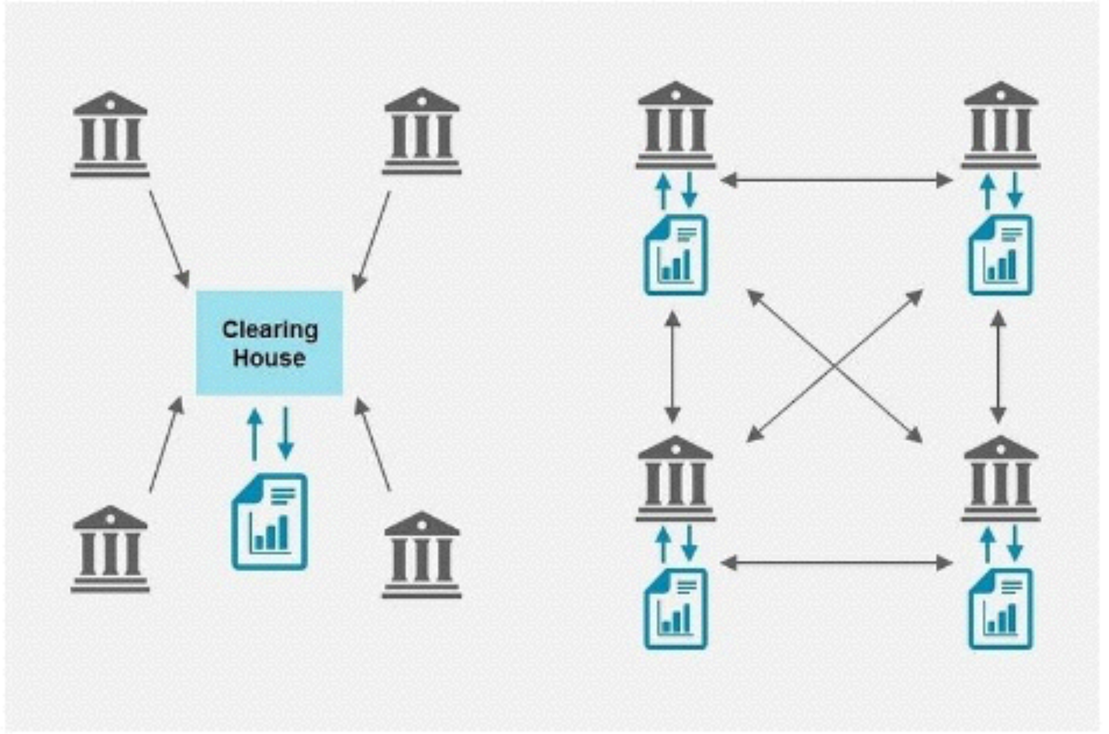


Technical basement

1. Decentralized and public ledger
2. Accounts (Keys)
3. Transactions
4. Blocks
5. Consensus
6. Miners

1/ Decentralized ledger

- All transactions and balances are public
  - Everybody knows if a payment can be done or not



2/ Accounts

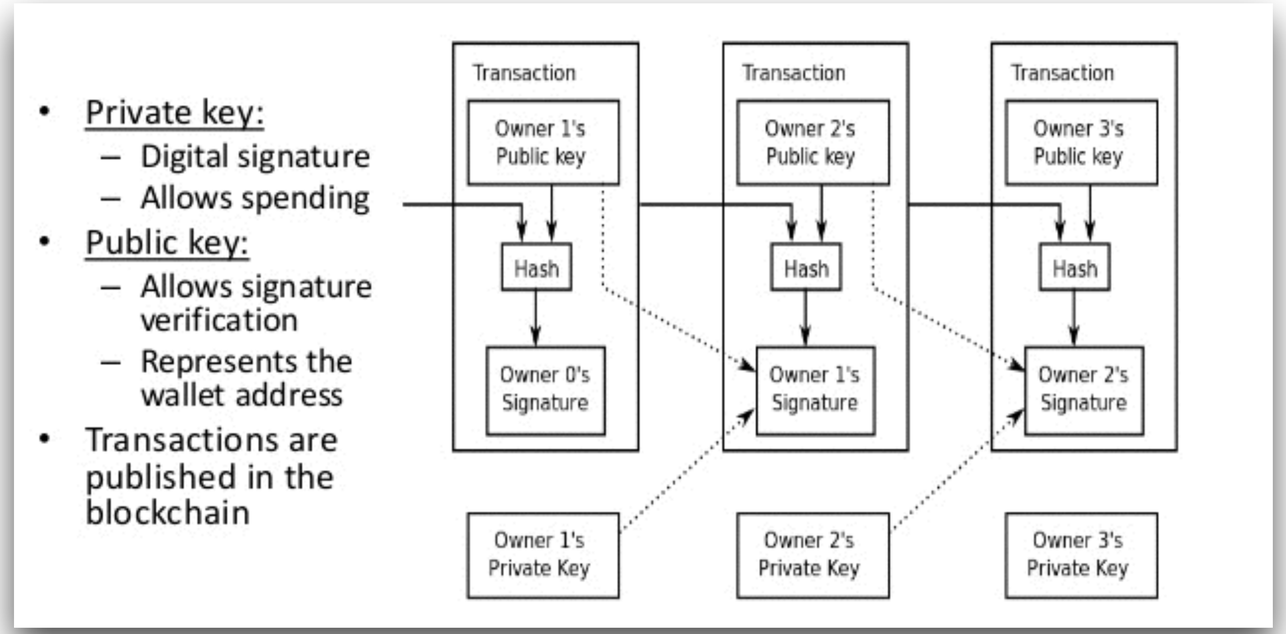
- Pair of Private / Public keys to identify the sender
- Private Key is 2^{256} bits, generated randomly
- Account => address

```
01111000101001010100101010011001010000011010010110000
01100010100101010010101110000101000001101001000110010
10001010011011001010111000011011000110101010011001100
00101001010100101011011001101001111010001101100101100
10100101010010101110000100110001101001000111010
```

5KCAskKGPWD4TaugT37og3wiNWBR8MdZkAnJQM8y6CzLkyAvoE9

3/ Transactions

- Tx = sender + receiver + amount
- Sender creates and signs transaction
- transactions are verified to avoid double-spend

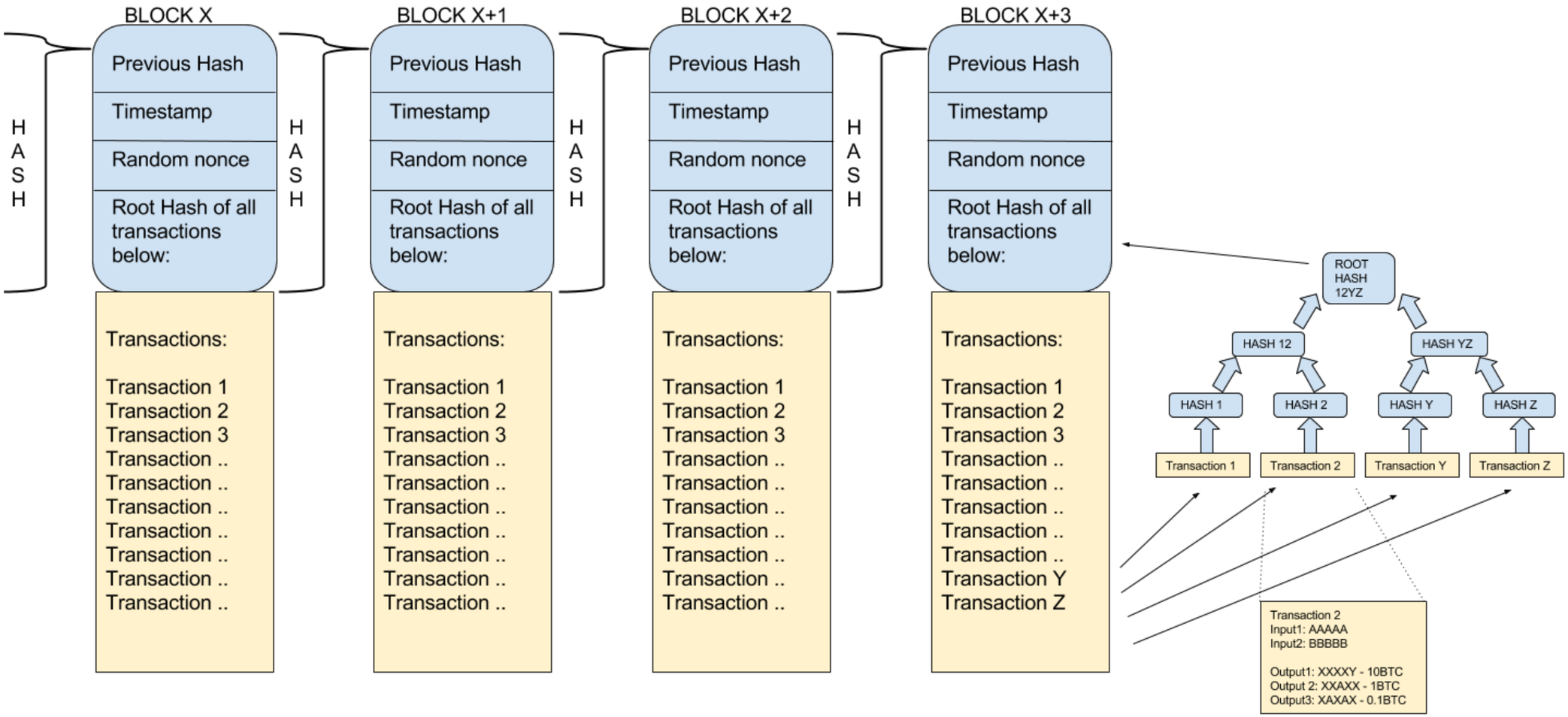


A transaction cannot be cheated

4/ Blocks

- Contains several transactions, in a merkle tree
- Are linked in a « chain »
- Consensus defines the rules to generate a block
- Content is not encrypted / is public

4/ Blocks


BLOCK X
BLOCK X+1
BLOCK X+2
BLOCK X+3
HASH
HASH
HASH
HASH
Previous Hash
Timestamp
Random nonce
Root Hash of all transactions below:
Transactions:
Transaction 1
Transaction 2
Transaction 3
Transaction ..
Transaction ..
Transaction ..
Transaction ..
Transaction ..
Transaction ..
Transaction ..
Transaction Y
Transaction Z
ROOT HASH 12YZ
HASH 12
HASH YZ
HASH 1
HASH 2
HASH Y
HASH Z
Transaction 1
Transaction 2
Transaction Y
Transaction Z
Transaction 2
Input1: AAAAA
Input2: BBBBB
Output1: XXXXY - 10BTC
Output 2: XXAXX - 1BTC
Output3: XAXAX - 0.1BTC

5/ Consensus

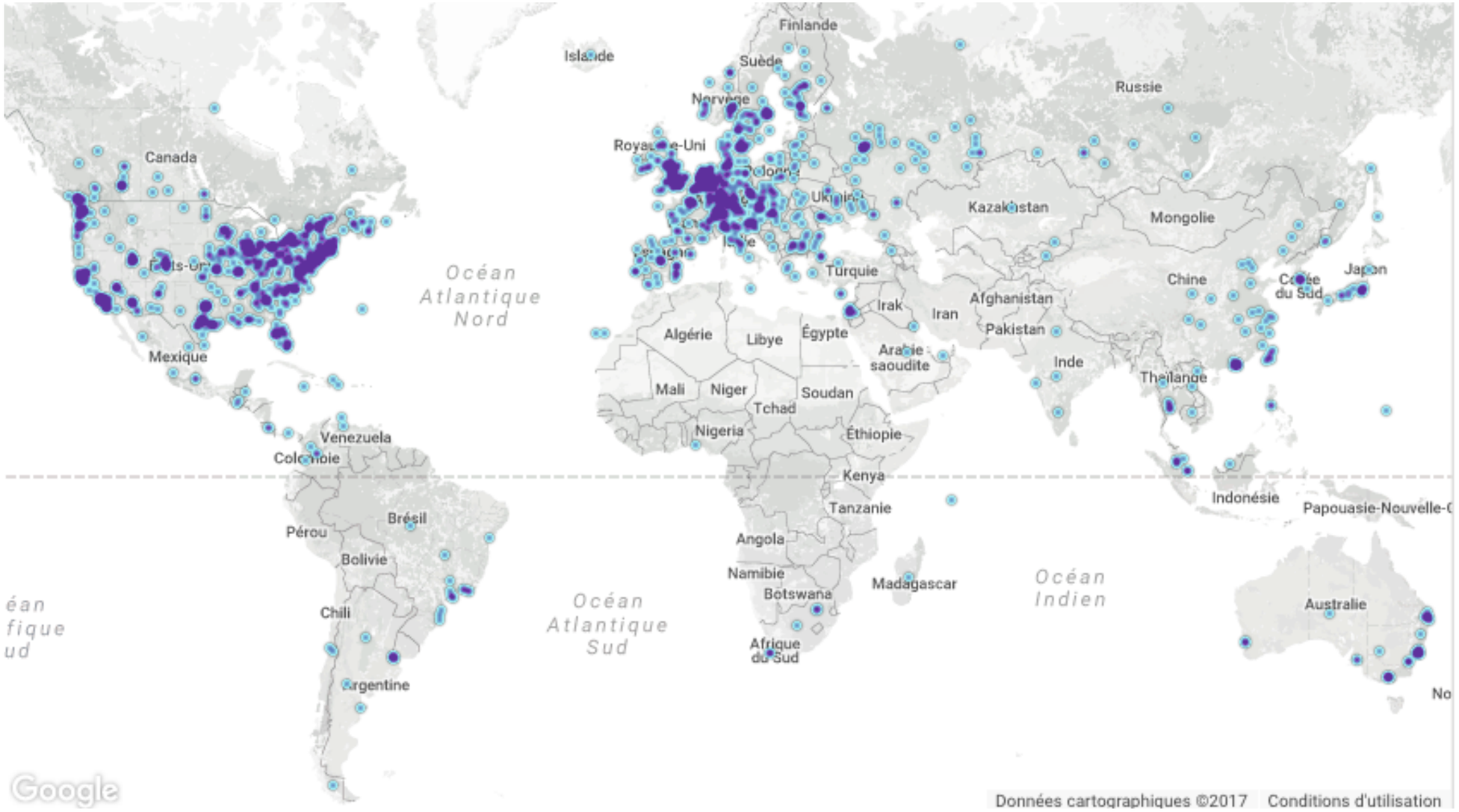
- Proof-of-Work (PoW)
  - Each nodes/miners accept the new situation based on that it has required some work to be done, and is cryptographically true
  - Random nonce => hash (256 bits) => challenge to find a number with some leading zeros
  - Each miner is incentivized : bitcoins rewarded for 1 block found

6/ Miners

+100’000 miners worldwide (estimated)

France +500

source : bitnodes.21.co



Going further !

What if ?

Other use cases

- Crypto-currencies, but not only !
- Assets issuance, crowdfunding, domain registration, title registration, gambling, precision market, internet of things, voting, intellectual property, logistics, tracking, distributed calculus,…… hundreds !
- Problem : bitcoin-like blockchain are limited to transaction handling

Introducing : Smart Contracts

General purpose programs

- **Runs** on each blockchain nodes —> resilient
- Code is **stored** on the blockchain —> can’t be modified
- Is **Turing - complete** —> conditions, loops, etc…
- **State** is stored on the blockchain —> history of tx cannot be changed
- Is **deterministic** —> tx affect state, can be determined accurately, history can be verified (note : pb with random number generation, pb with external calls)

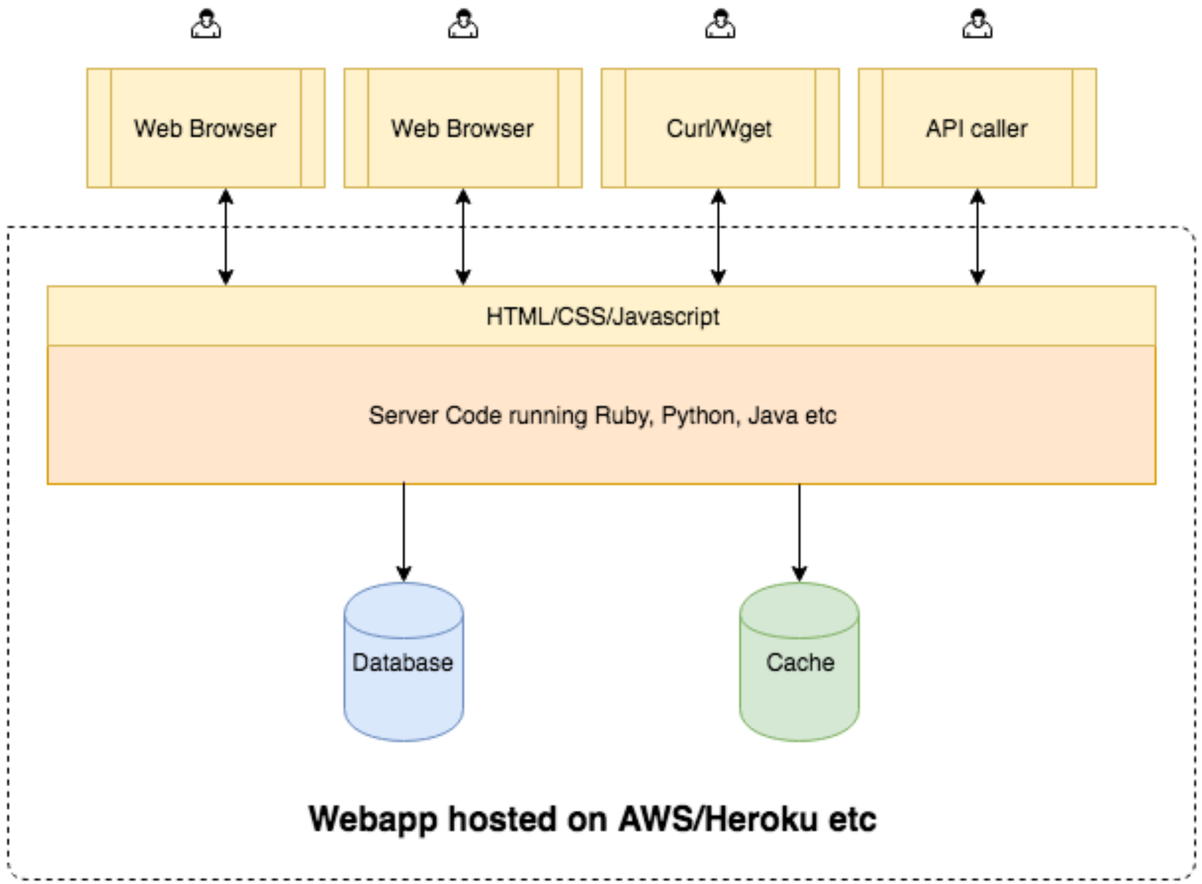
Ethereum

« Smart contracts »
technology

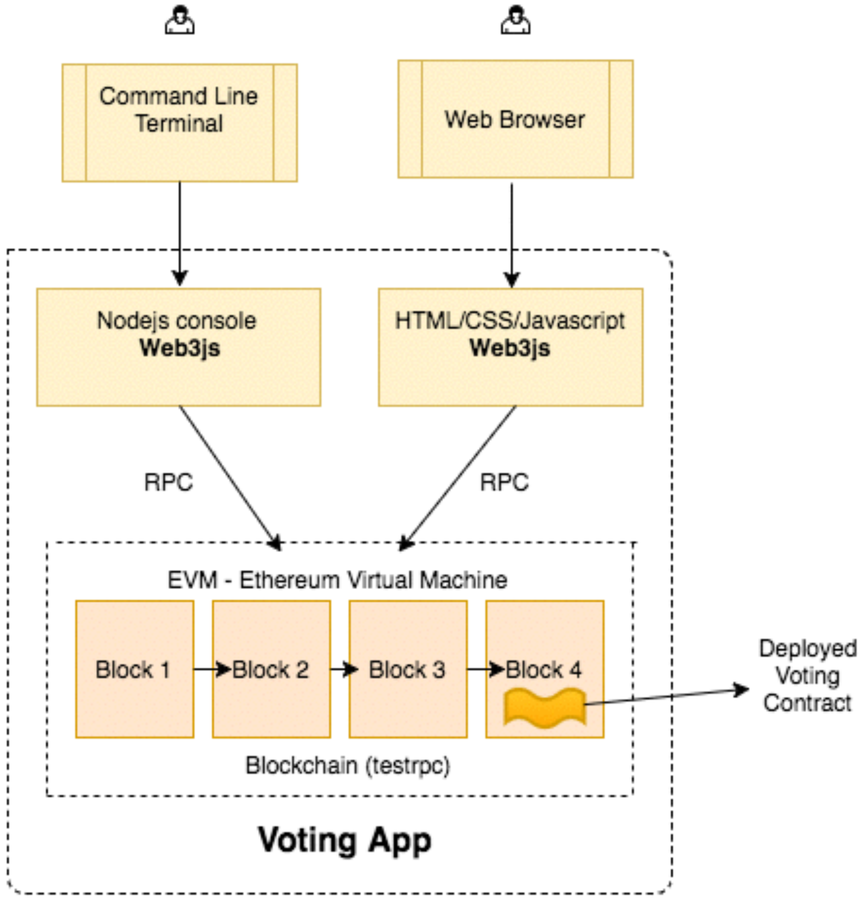
Ethereum

- The most widely used, simple to use and develop
- Similarities with Bitcoin : PoW, miners incentivized with ether
- Add Smart Contracts
  - High - level language : solidity (javascript-like),
  - Virtual machine (EVM) : somewhat like JVM

Ethereum : application layers and APIs

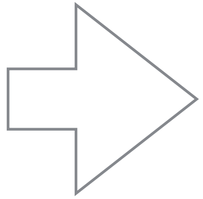


VS



Traditional

Decentralized on blockchain




NOKIA
NOKIA


9:41 AM
100%
Messages
Calendar
Photos
Camera
Weather
Clock
Maps
Videos
Notes
Reminders
Stocks
News
Health
iTunes Store
App Store
Settings
Phone
Safari
Mail
Music

Other implementations

- **Hyperledger** fabric (IBM) : private chain
- **Corda** (R3 consortium) : financial services
- **Zcash** : privacy on public chain (Zero-knowledge-proof)
- …hundreds others !

In a nutshell

Core Concepts

- **Blocks, Transactions, Nodes**
- **Crypto toolbox**
- **Merkle trees** & **Hashes**
- **Consensus Algorithm**
- **P2P**, **Decentralized, Distributed**
- **Programming Language**

Analysis : Information classification

- « **Confidentialité** » : problem here because data is not encrypted.
- « **Intégrité** » : once information is in a block, it cannot be modified or reverted, never.
- « **Disponibilité** » : information is always available, relaying on thousand nodes worldwide.
- « **Traçabilité** » : every transaction is stored and visible on the blockchain, senders and receiver are known

Some Limits

- **Privacy** : all transactions are visible
- **Performance** : number of tx/s
  - No vertical or horizontal enhancement possible
  - Time needed to create a block + number of tx per block

What about us ?


I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
E-mail: SCOTTADAMS@AOL.COM
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.
© 1995 United Feature Syndicate, Inc.(NYC)

Mistakes to avoid in your project

- **Not understanding** or ignoring **the objective** of blockchain technology
- Considering actual technology is **ready for a wider** use
- Mistaking a kind of basic and **limited protocol** with a complete **business-ready** solution
- Taking blockchain as **just a database** or storage mechanism
- Thinking **actual leader** platforms will still be in the future
- Consider smart contract technology is **like standard programming**
- Ignoring **governance** issues in a peer-to-peer network
- Skip **learning process**

source : lemondeinformatique.fr

Thank you.