



SOFT**INSTIGATE**

On Business Models in the Crypto Economy

Andrea Di Cesare
“De Cifris incontra Perugia”
16 October 2019



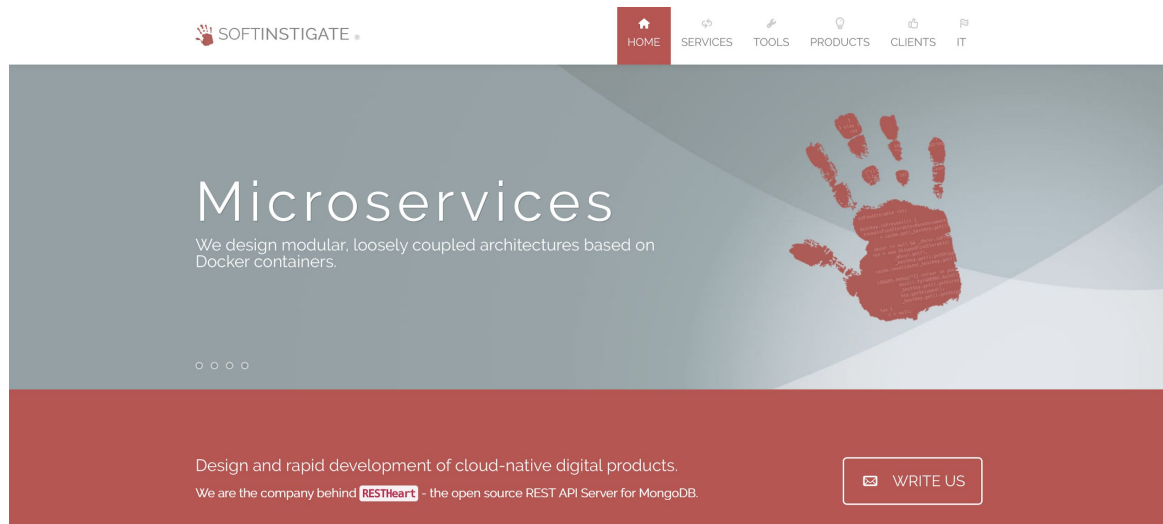
Soft**Instigate**

What we do

Soft**Instigate** is a software development firm est. 2005

focused on → **Product Lean Development** ←

with a strong know how on **software business models**



more at <https://softinstigate.com>



SoftInstigate

Research today to get ready for tomorrow

software development is a fast-paced, crazy and exciting world

no one of today's software trends { cloud, API, agile, microservices, mobile, SPA, IoT, Big Data, ... } were there 10 years ago

→ Continuous Research is mandatory ←



Centerless.io

{ Blockchain | Smart Contracts | Digital
Assets } Lab

Centerless.io deals with the research and development of new solutions in the field of *Blockchain technologies*, in the assumption that these will allow the realization of the next generation of disruptive products.

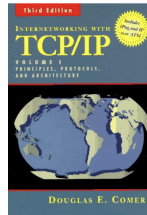


Blockchain R&D Lab

we study the blockchain technology, looking for an answer to the **core question**:

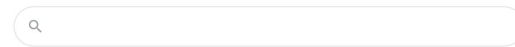
*which will be the blockchain **killer app**?*

In 1994 I was reading this....



Internetworking with TCP/IP
Douglas E. Comer

...and I should have guessed this!



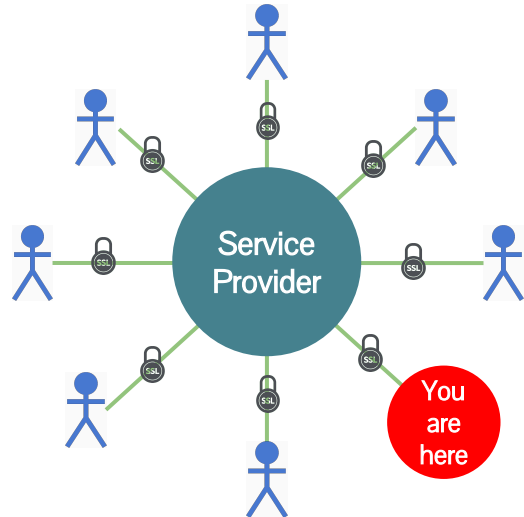
And on 31 October 2008 **Satoshi Nakamoto** posted the paper “*Bitcoin: A Peer-to-Peer Electronic Cash System*” → promising a yet new paradigm shift... ←

The Web is fueled by Cryptographic Technologies

Cryptography shaped the Web as we know it today and is likely to disrupt it again

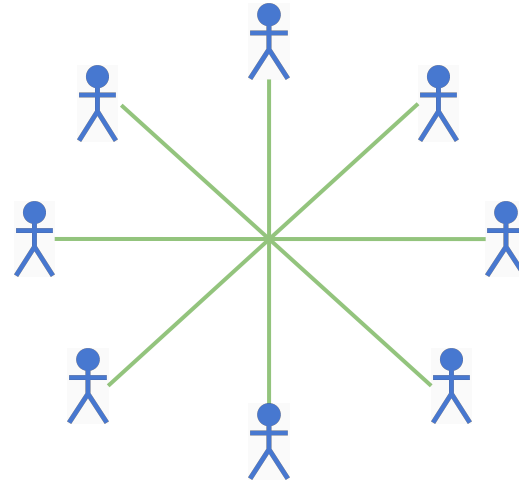
Web 2.0

services enabled by **secure**
communication channels
over an insecure network



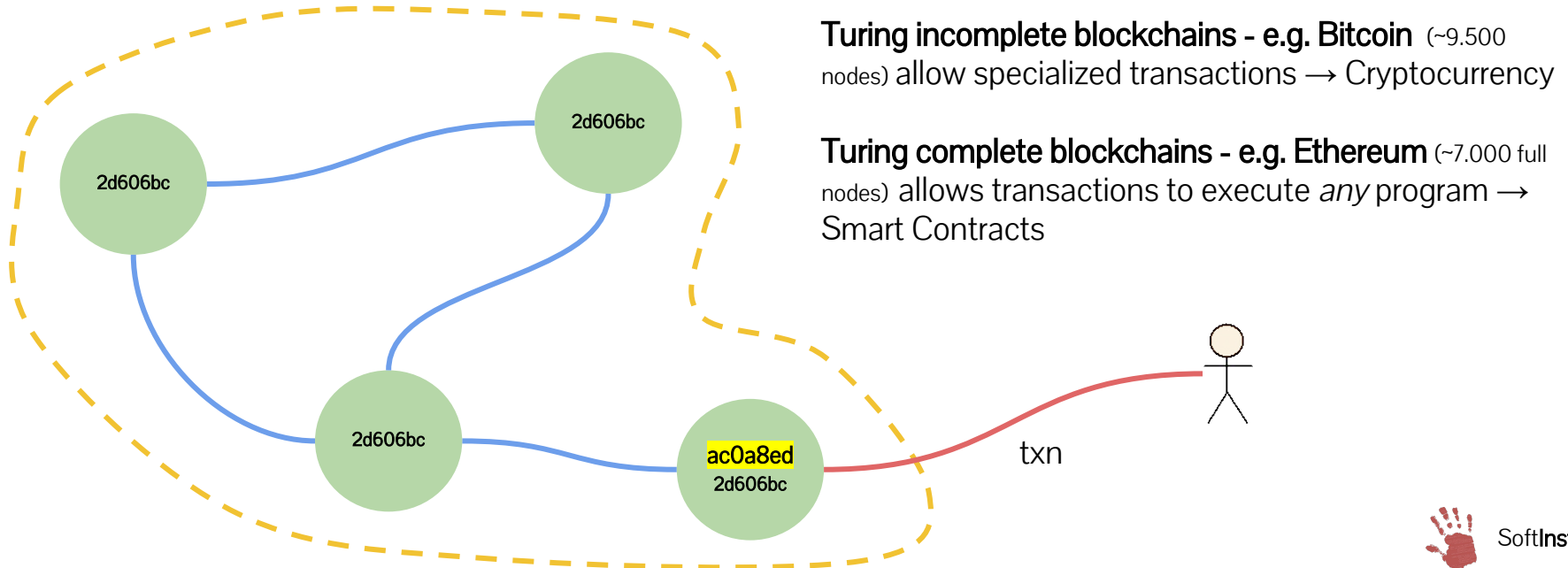
Web 3.0

services enabled by **secure** and
distributed network



Blockchain as a distributed system

A blockchain is a distributed network that ***automatically*** reaches *global consensus* on local state changes with *Byzantine Fault Tolerance*.



Smart contracts

[OpenZeppelin Ownable.sol contract snippet](#)

Smart Contracts are programs executed by the Blockchain.

Interesting! Solidity, the contract-oriented programming language proposed by Gavin Wood, CTO of Ethereum, uses the keyword *contract* where other object-oriented languages use *class*.

An ERC20 Token (cryptocurrency) can be implemented in Solidity with few lines of code!

On 8/10/2019 217.459 Token Contracts.

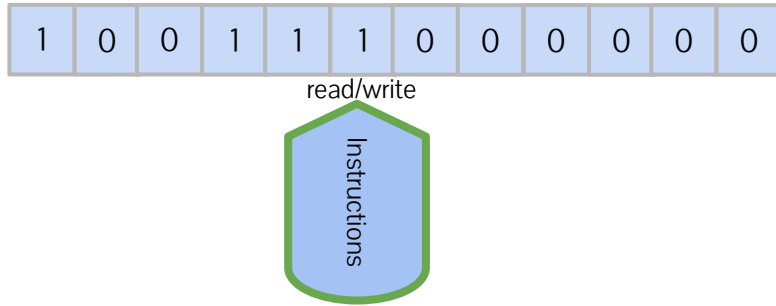
```
78 lines (68 sloc) | 2.35 KB
Raw Blame History
1 pragma solidity ^0.5.0;
2
3 import "../GSN/Context.sol";
4 /**
5  * @dev Contract module which provides a basic access control mechanism, where
6  * there is an account (an owner) that can be granted exclusive access to
7  * specific functions.
8  *
9  * This module is used through inheritance. It will make available the modifier
10  * `onlyOwner`, which can be applied to your functions to restrict their use to
11  * the owner.
12  */
13 contract Ownable is Context {
14     address private _owner;
15
16     event OwnershipTransferred(address indexed previousOwner, address indexed newOwner);
17
18     /**
19      * @dev Initializes the contract setting the deployer as the initial owner.
20      */
21     constructor () internal {
22         address msgSender = _msgSender();
23         _owner = msgSender;
24         emit OwnershipTransferred(address(0), msgSender);
25     }
26
27     /**
28      * @dev Returns the address of the current owner.
29      */
30     function owner() public view returns (address) {
31         return _owner;
32     }
33 }
```

contract Ownable is Context {

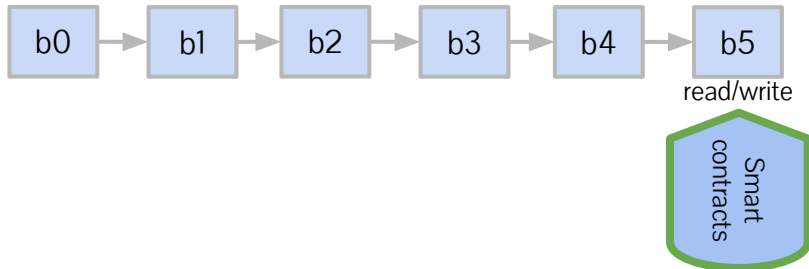


The World Computer

A **Turing machine** is an abstract machine which manipulates symbols stored in the cells of a tape according to the instructions set.



A **blockchain** is machine which manipulates the data stored in a sequence of blocks according to smart contracts



The blockchain as a
distributed turing machine!



**Blockchain as
the World Computer**

The features of the World Computer

The World Computer

- provides Computation Power and Storage
- allows users/smart contracts to receive and send *messages*
- is intrinsically secure
- handles User (crypto) Identities → Identity = Public Key
- allows users/smart contracts to receive and send *money*
- is transparent → users can read any data on the blockchain, including the code of smart contracts
- using the World Computer is expensive (e.g. storage costs ~ €70.000/GB¹)
- The World Computer is (currently) slow ~ 25 TPS



Vitalik Non-giver of Ether
@VitalikButerin

9. Blockchains of the future with proof of stake and sharding will be thousands of times more efficient, and so the efficiency sacrifices of putting things on a chain will become more and more acceptable.

358 6:11 PM - Dec 10, 2018

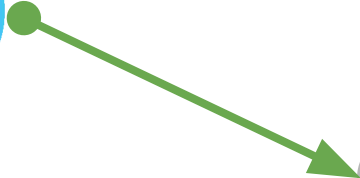


1) See question on etheruem.stackexchange.com: [What is the cost of storage on Ethereum?](#)



Web 2.0 Business Models in a Picture

Users interact with Services
via Mobile or Web Application



API



Service
Provider

- **Google** → service to search web sites
- **MyBank** → service to execute wire transfers
- **Uber** → service to call and pay taxi rides
- **AirBnB** → service to book and pay hotel rooms

- Develops the Service
- Manages the Infrastructure
- Enforces Security
- Manages User Identity
- Handles Payments



Users are willing to pay fees to Service
Providers because they develop and securely
run Complex Systems that simplify their life.



The impact of decentralization

What if a service runs on the World Computer?

→ **Everything changes** ←

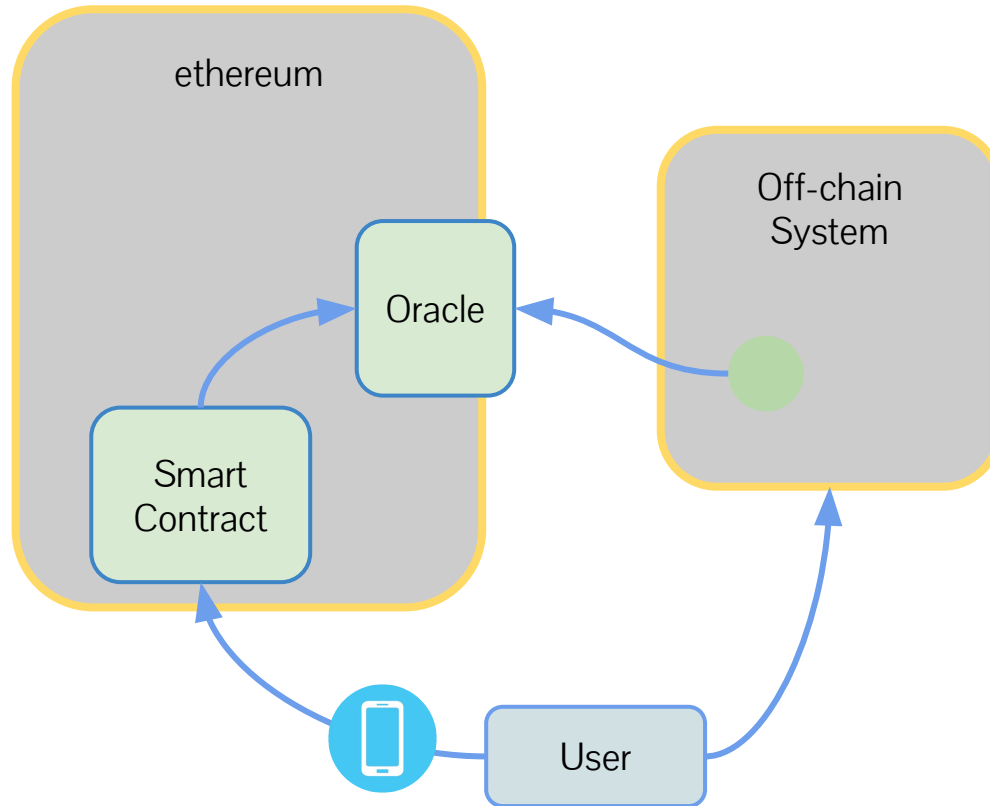
- Develops the Service
- ~~Manages the Infrastructure~~
- ~~Enforces Security~~
- ~~Manages User Identity~~
- ~~Handles Payments~~

Code can be read and replicated by anybody

These are out-of-the-box features of the World Computer



Web 3.0 Business Models in a Picture



Users don't interact directly with smart contract as they don't interact with APIs → **Great UX makes the difference**

Off-chain systems are needed in most of the cases unless process runs completely in chain → **add value to the service and keep it under control of the provider**



Hybrid in-chain and off-chain systems that leverage the blockchain features, e.g. for trust

The perfect example: cryptokitties.co

Leverages blockchain unique features ✓

- Crypto kitties are unique (virtual kitties are non fungible tokens)
- Users really own them in their wallet (no chance to double spend it)
- Traded via smart contracts (reverse auctions to lower costs)
- Use Ether, not yet another cryptocurrency (custom tokens are the kitties)
- User Identity is its Ethereum account (no need for yet another sign-up)

Great UX ✓

- Just needs a Browser with Metamask wallet plugin
- Great Web UI

Integrated with Off-chain systems ✓

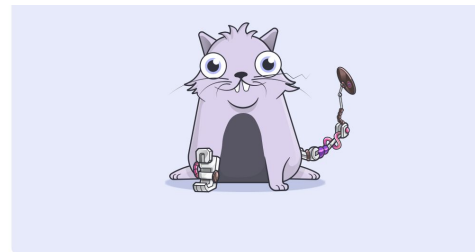
- The off-chain system visualizes the tokens, without it kitties are just DNA!

So successful that pushed Ethereum capacity to its limits ¹

¹) See BBC article [CryptoKitties craze slows down transactions on Ethereum](#)

CryptoKitties

Collect and breed furrever friends!

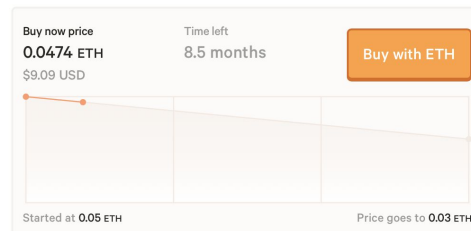


fileshare #572

1619380 X Gen 17 ⌚ Sluggish Cooldown (4d)



Not in any Collection

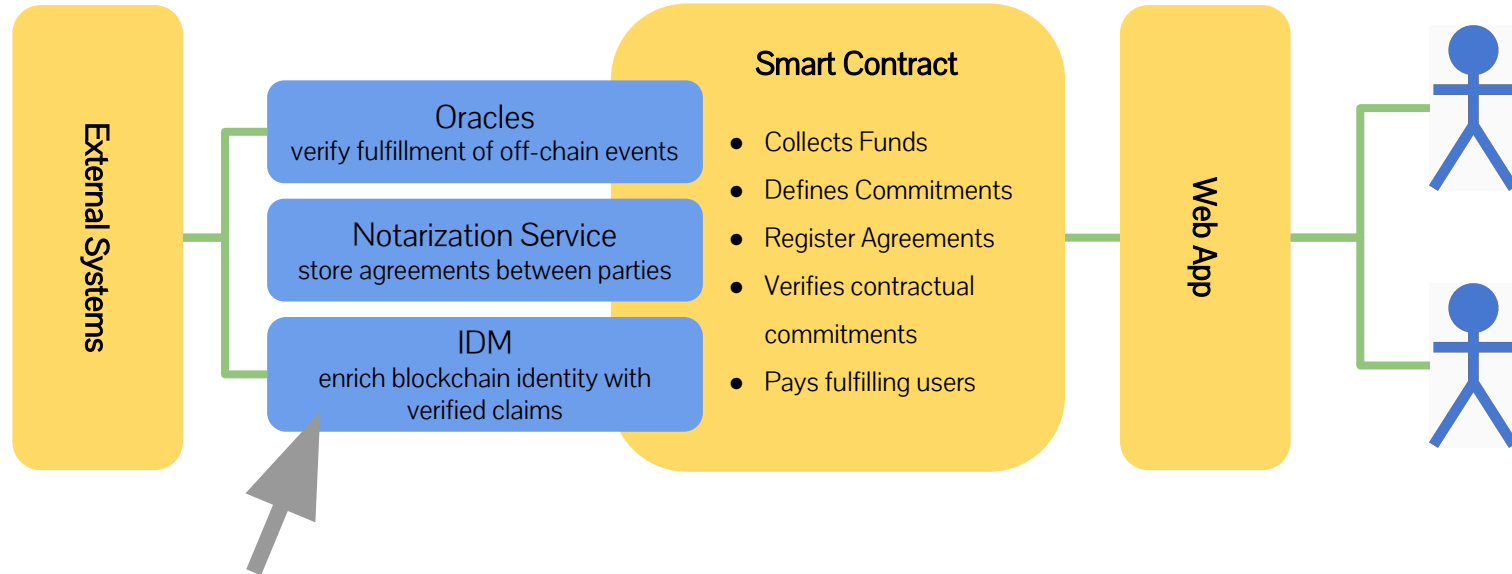


SoftInstigate

What we are working on....

Service that pays who fulfills contractual commitments as verified on online systems

A simple example: get paid clicking *Like* below a given post on Facebook



Questions?

Contacts



SOFT**INSTIGATE**

Web	https://softinstigate.com
Email	info@softinstigate.com
Twitter	https://twitter.com/softinstigate
LinkedIn	https://linkedin.com/company/softinstigate

Via G. D'Annunzio 28, 67100 L'Aquila, Italy
Via Copernico 38, 20125 Milano, Italy



Soft**Instigate**