



ΑΠΟΚΕΝΤΡΩΜΕΝΕΣ ΕΦΑΡΜΟΓΕΣ

ΑΝΑΠΤΥΞΗ ΠΛΑΤΦΟΡΜΑΣ ΕΠΙΚΥΡΩΣΗΣ ΑΚΑΔΗΜΑΪΚΩΝ ΕΓΓΡΑΦΩΝ
ΠΑΝΩ ΣΕ BLOCKCHAIN

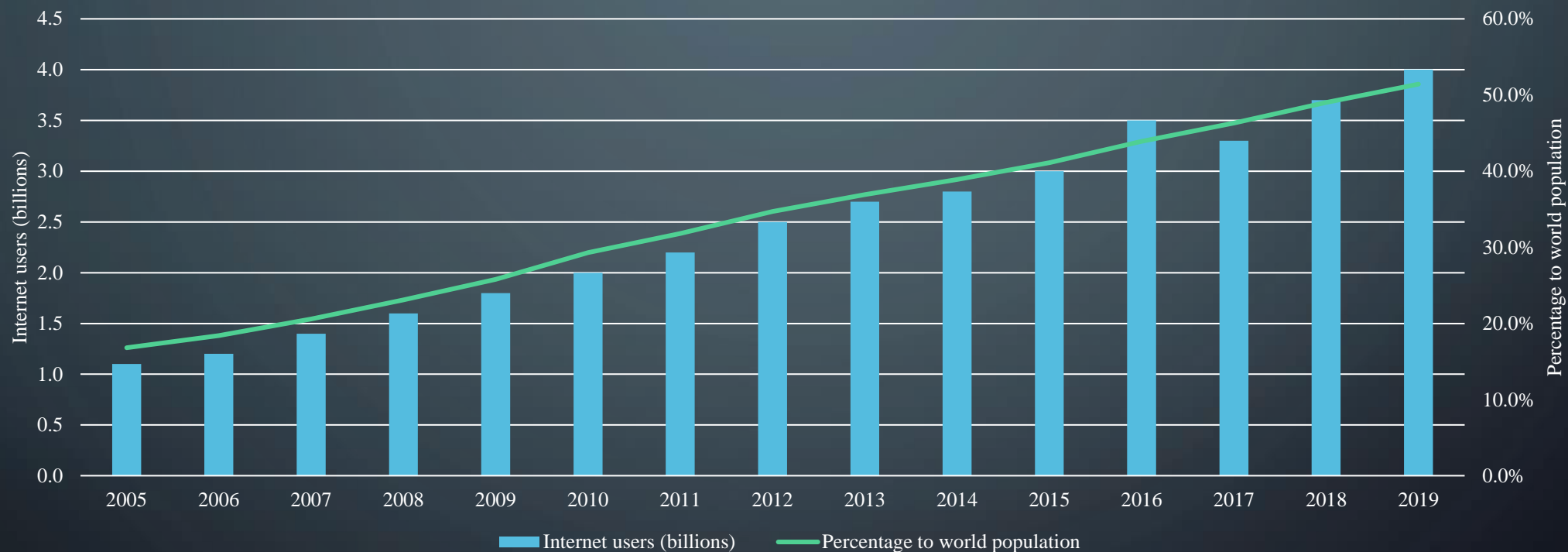
Μαργαρίτης Αργύριος – mai19040

Πρόγραμμα Μεταπτυχιακών Σπουδών
Τμήμα Εφαρμοσμένης Πληροφορικής
ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΛΙΓΑ ΛΟΓΙΑ ΓΙΑ ΤΗΝ ΕΡΓΑΣΙΑ...

- Εκπόνηση: Ιούλιος 2020 - Αύγουστος 2021
- Περιεχόμενα:
 - Θεωρητικό υπόβαθρο
 - Κρυπτογραφία
 - Blockchain
 - Smart Contracts
 - Decentralized Applications
 - Ανάπτυξη αποκεντρωμένης εφαρμογής
 - Demo case: Επικύρωση ακαδημαϊκών εγγράφων
 - CryptoCerts

ΤΟ ΔΙΑΔΙΚΤΥΟ ΣΗΜΕΡΑ



Η χρήση του διαδικτύου από το 2005

Πηγή: International Telecommunication Union (ITU)

CENTRALIZATION

- Tech giants

- FAAMG (Facebook, Amazon, Apple, Microsoft και Alphabet)
- 22% του δείκτη S&P 500

- Μοντέλο client – server

- Κέντρο όλων ο server
- Τεράστια racks σε γιγάντια data centers



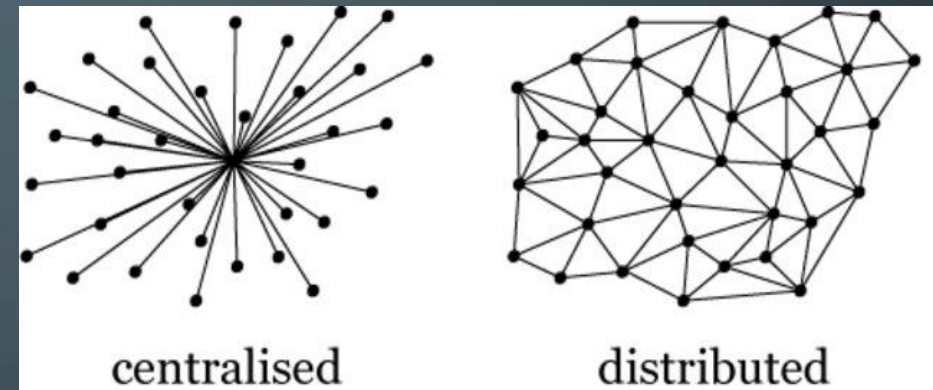
Στρέβλωση στην ισορροπία Χρήστη – Πλατφόρμας

- Αποτελέσματα

- Outages (Facebook 4/10/2021, Google 14/12/2020, κτλ.)
- Δεδομένα και ιδιωτικότητα χρηστών (Cambridge Analytica, Equifax 2017, κτλ.)
- Έλλειψη ελέγχου

WEB3 - ΑΠΟΚΕΝΤΡΩΜΕΝΟΣ ΙΣΤΟΣ

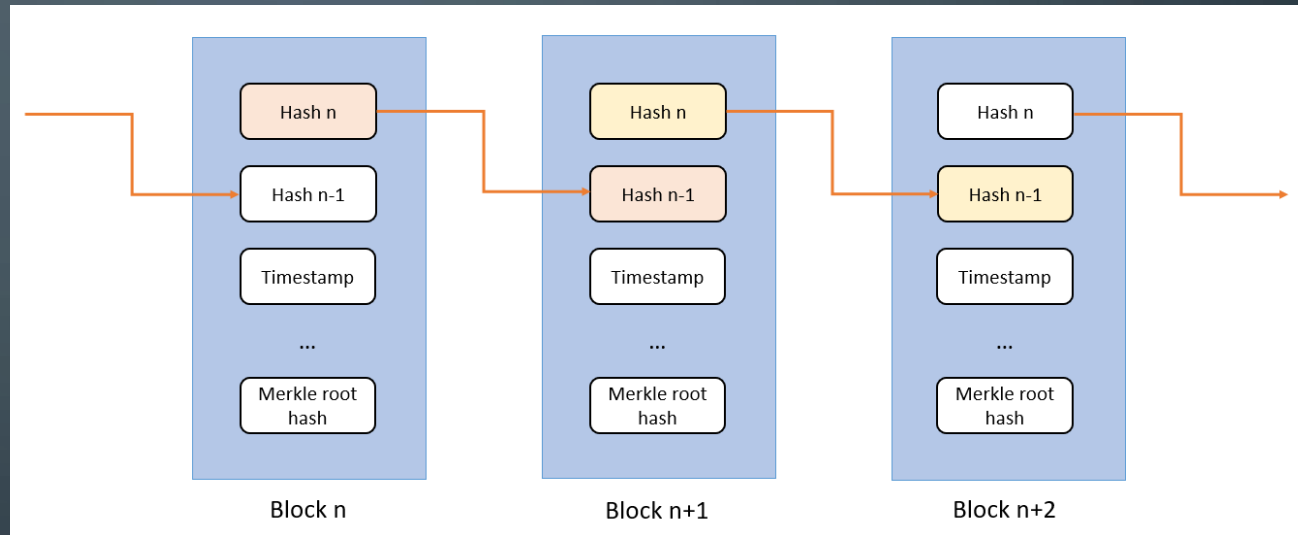
- Μοντέλο peer-to-peer (P2P)
 - Napster (1990s)
 - BitTorrent (2000s)
- Πλεονεκτήματα
 - Βελτιστοποίηση χρήσης πόρων (efficiency)
 - Ανθεκτικότητα (resilience)
 - Διαθεσιμότητα (availability)
 - Επεκτασιμότητα (scalability)
- Εφαρμογή σε ιστοτόπους και web εφαρμογές
- Stateful vs Stateless



Η διαφορά μεταξύ των
αρχιτεκτονικών

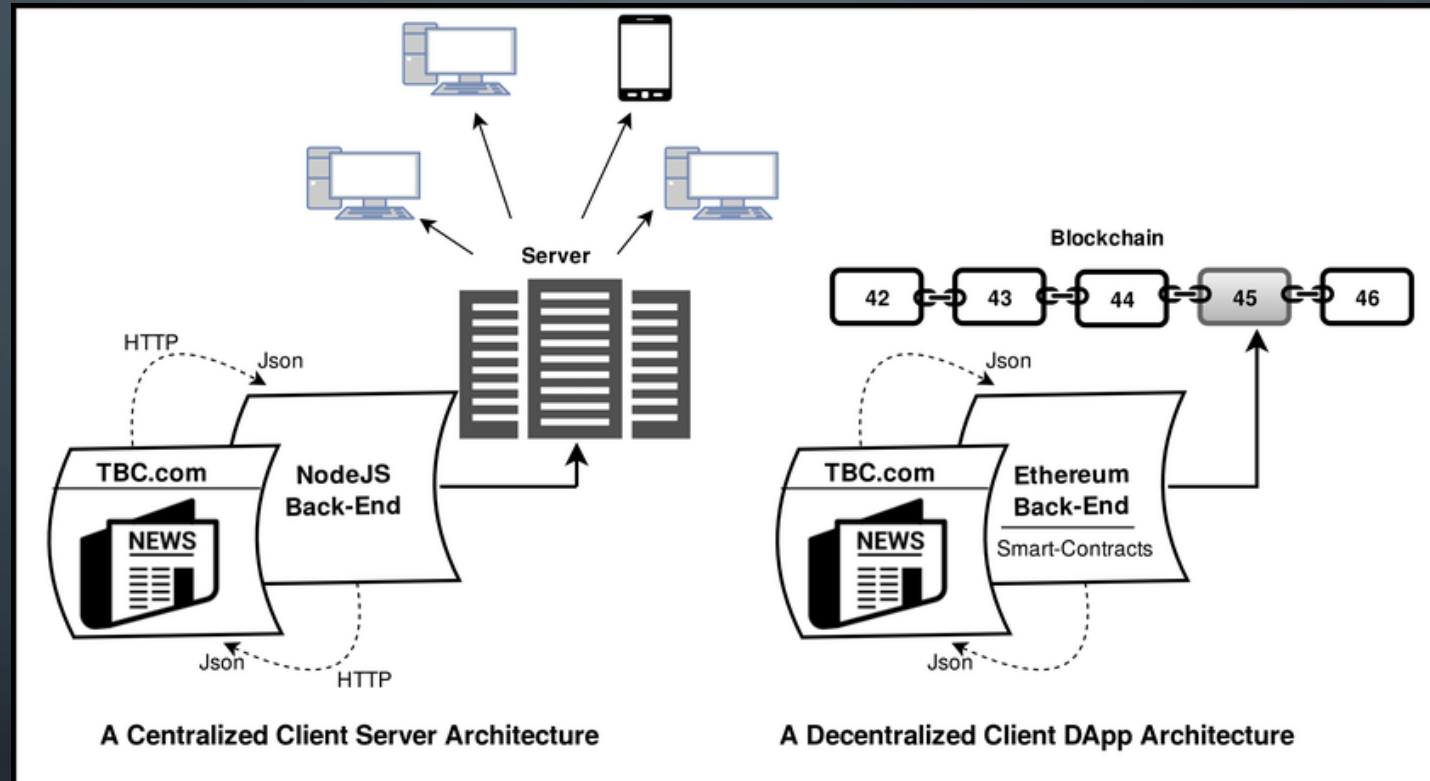
DECENTRALIZED APPLICATIONS

- Εν συντομία dapps
- Κρυπτογραφία
 - Public key cryptography
 - Digital signatures
 - Hash functions
- Blockchain
 - Bitcoin (2009)
 - Κατανεμημένη βάση δεδομένων
- Smart contracts
 - N. Szabo (1994)



Βασική δομή ενός blockchain

DECENTRALIZED APPLICATIONS - ΑΡΧΙΤΕΚΤΟΝΙΚΗ



Σύγκριση αρχιτεκτονικών web app και dapp

Πηγή: S. Sayeed, H. Marco-Gisbert και T. Caira

CRYPTOCERTS DAPP DEVELOPMENT

- Ethereum

- V. Buterin (2013)
- Solidity (Turing-complete language)



- Interplanetary File System (IPFS)

- Κατανεμημένο σύστημα αρχείων



- Web3.js – MetaMask

- Διασύνδεση frontend με το blockchain

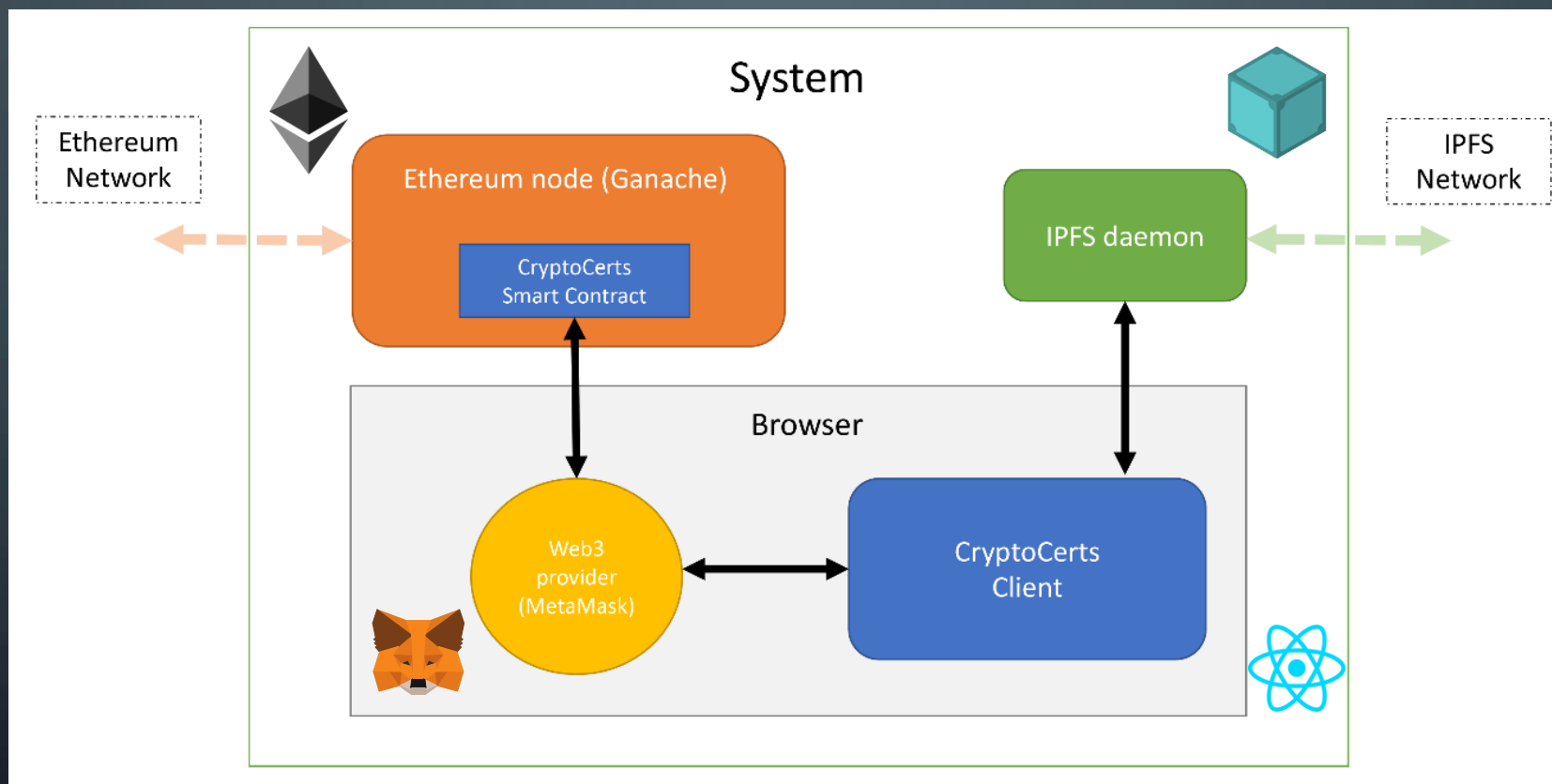


- React

- Facebook



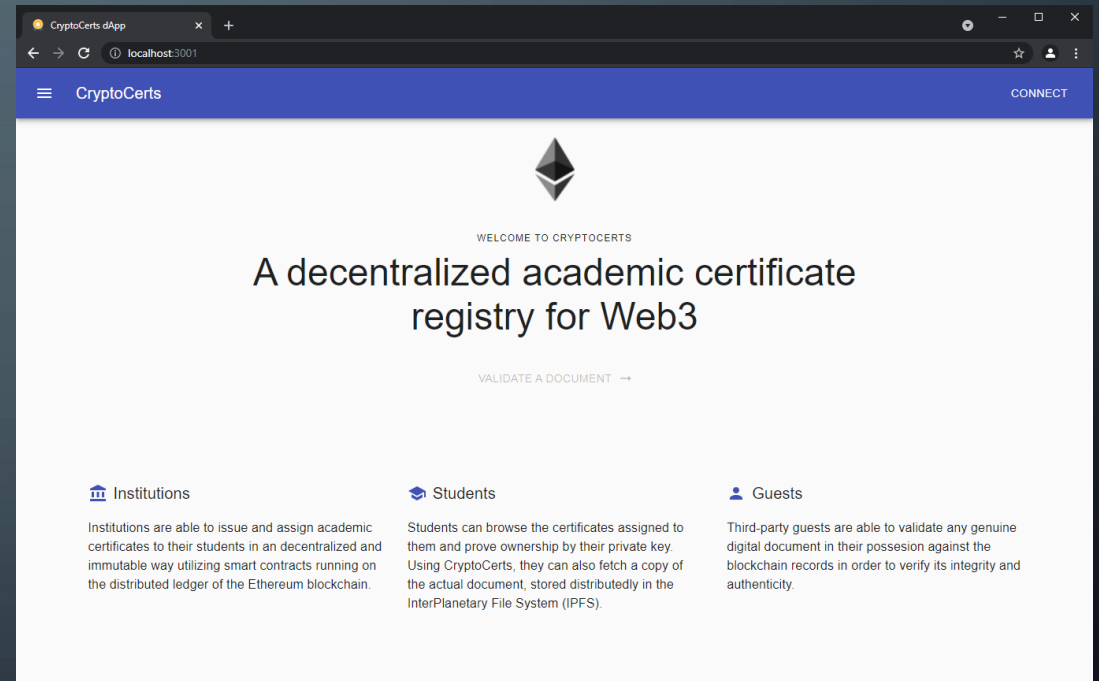
CRYPTOCERTS – Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ



Η αρχιτεκτονική της αποκεντρωμένης εφαρμογής CryptoCerts

CRYPTOCERTS – Η ΠΛΑΤΦΟΡΜΑ

- Οντότητες
 - Administrator
 - Διαχείριση των Institutions
 - Institutions
 - Διαχείριση των Certificates
 - Students
 - Λήψη και επαλήθευση των Certificates
 - Guests
 - Επαλήθευση των Certificates



Η αρχική σελίδα του CryptoCerts

CRYPTOCERTS INSTITUTION FACTORY CONTRACT

```
1 // SPDX-License-Identifier: UNLICENSED
2
3 pragma solidity ^0.7.0;
4
5 import "../node_modules/@openzeppelin/contracts/access/Ownable.sol";
6
7 contract InstitutionFactory is Ownable {
8     event InstitutionCreated(
9         uint256 indexed id,
10         string name,
11         address indexed addr
12     );
13
14     struct Institution {
15         string name;
16         string location;
17         bool isValid;
18     }
19
20     mapping(address => uint256) public ownerToInstitution;
21     mapping(uint256 => address) public institutionToOwner;
22
23     Institution[] public institutions;
24
25     /**
26      * @dev Throws if called by any account who doesn't belong to an Institution.
27      */
28     modifier onlyInstitution() {
29         require(
30             ownerToInstitution[_msgSender()] != 0,
31             "Caller is not an institution owner"
32         );
33         _;
34     }
```

```
35
36     function createInstitution(string memory _name, string memory _location, address _address) public onlyOwner {
37         institutions.push(Institution(_name, _location, true));
38
39         uint256 id = institutions.length;
40         ownerToInstitution[_address] = id;
41         institutionToOwner[id] = _address;
42
43         InstitutionCreated(id, _name, _address);
44     }
45
46     function editInstitution(uint256 _id, string memory _name, string memory _location) public onlyOwner {
47         institutions[_id].name = _name;
48         institutions[_id].location = _location;
49     }
50
51     function deleteInstitution(uint256 _id) public onlyOwner {
52         Institution memory institution = institutions[_id];
53         institution.isValid = false;
54         ownerToInstitution[institutionToOwner[_id]] = 0;
55         institutionToOwner[_id] = address(0);
56     }
57
58     function getInstitutionsCount() external view returns (uint256) {
59         return institutions.length;
60     }
61 }
```

Παράδειγμα ενός smart contract

BRACE YOURSELVES...



**KEEP
CALM
IT IS
DEMO
TIME**