
# ΑΠΟΚΕΝΤΡΩΜΕΝΕΣ ΕΦΑΡΜΟΓΕΣ

## ΑΝΑΠΤΥΞΗ ΠΛΑΤΦΟΡΜΑΣ ΕΠΙΚΥΡΩΣΗΣ ΑΚΑΔΗΜΑΪΚΩΝ ΕΓΓΡΑΦΩΝ ΠΑΝΩ ΣΕ BLOCKCHAIN

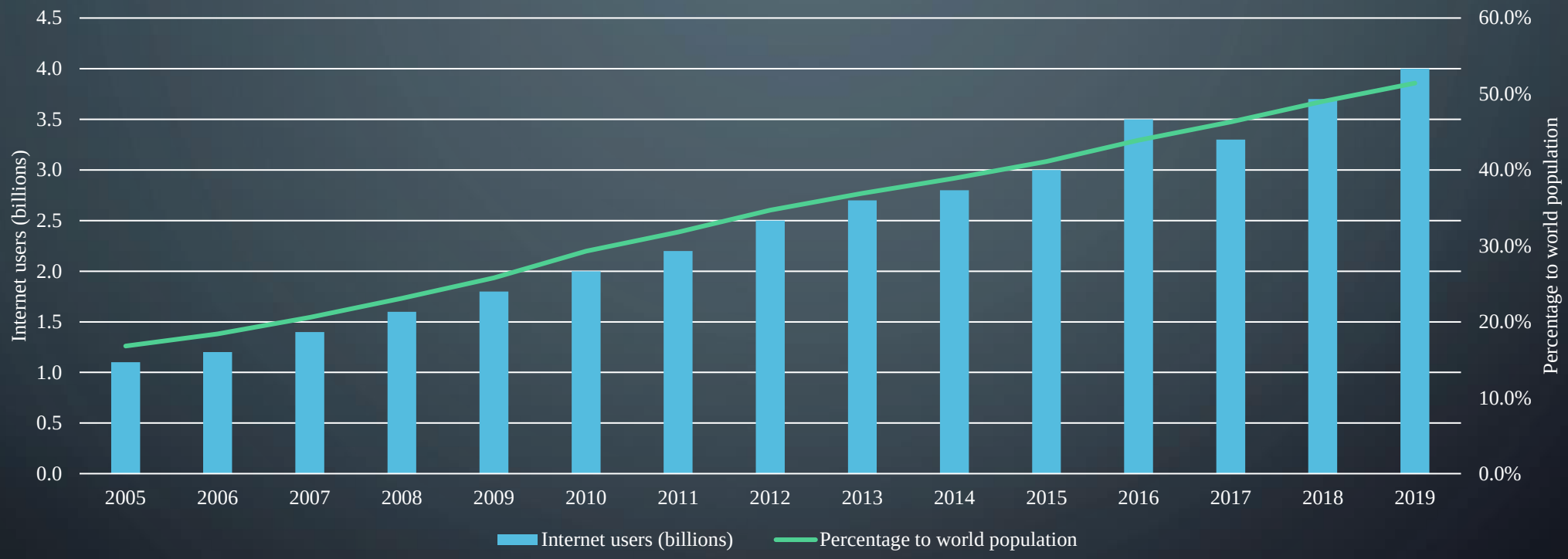
Μαργαρίτης Αργύριος – mai19040

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)

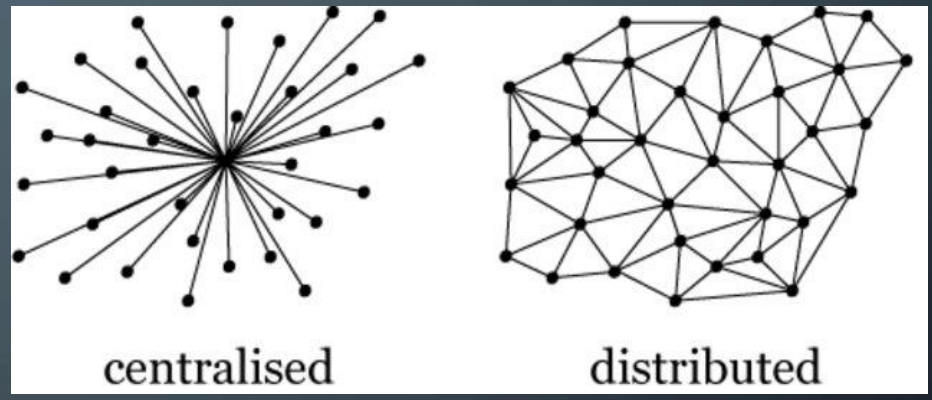
# CENTRALIZATION

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


Στρέβλωση στην ισορροπία Χρήστη – Πλατφόρμας

# WEB3 - ΑΠΟΚΕΝΤΡΩΜΕΝΟΣ ΙΣΤΟΣ

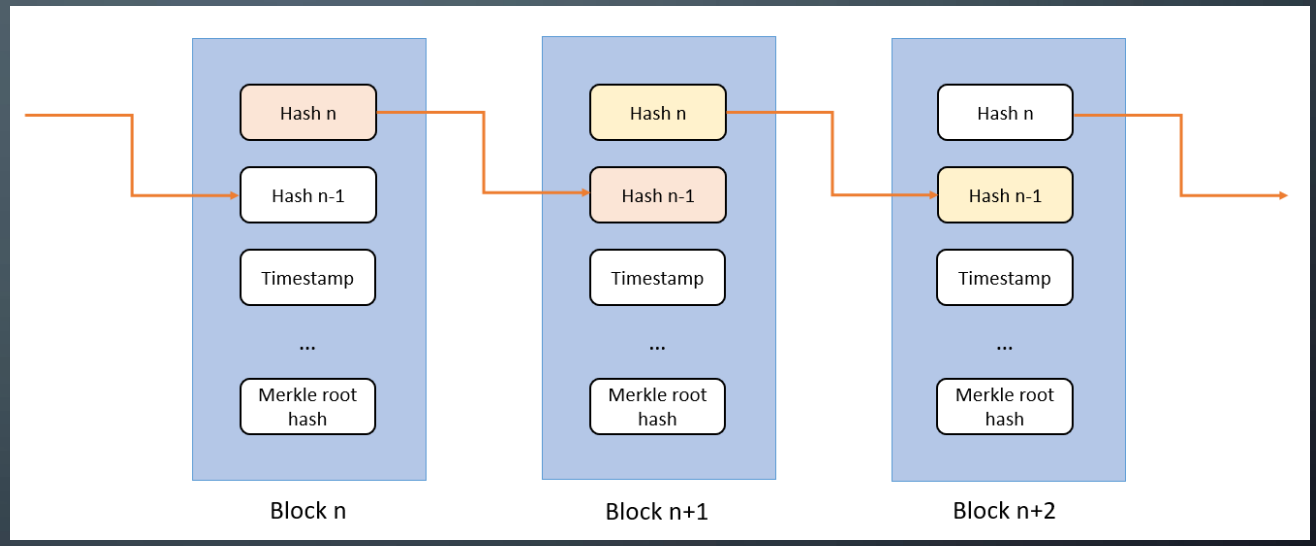
- Μοντέλο peer-to-peer (P2P)
  - Napster (1990s)
  - BitTorrent (2000s)
- Πλεονεκτήματα
  - Βελτιστοποίηση χρήσης πόρων (efficiency)
  - Ανθεκτικότητα (resilience)
  - Διαθεσιμότητα (availability)
  - Επεκτασιμότητα (scalability)
- Εφαρμογή σε ιστοτόπους και web εφαρμογές
- Stateful vs Stateless




Η διαφορά μεταξύ των αρχιτεκτονικών

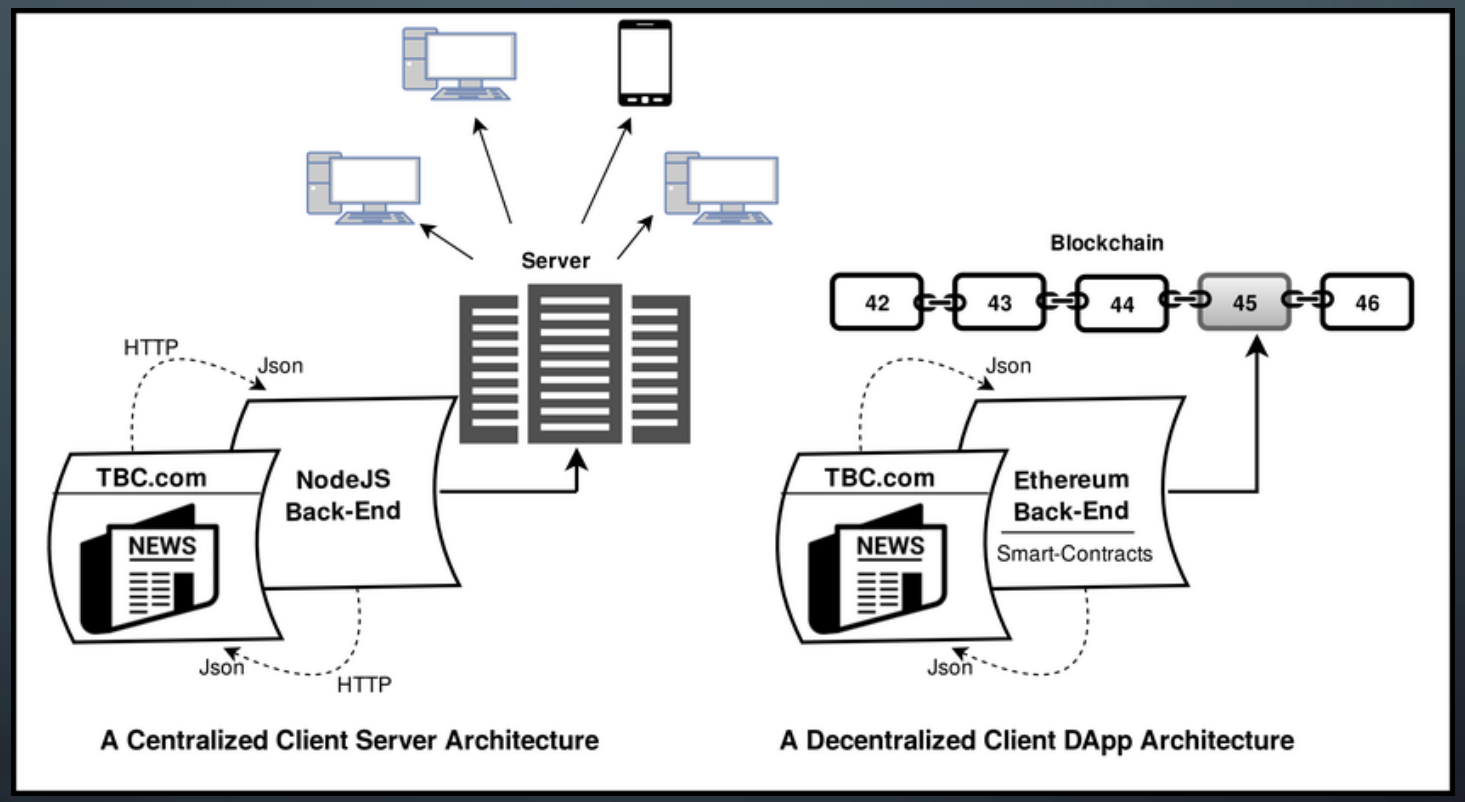
# DECENTRALIZED APPLICATIONS

- 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

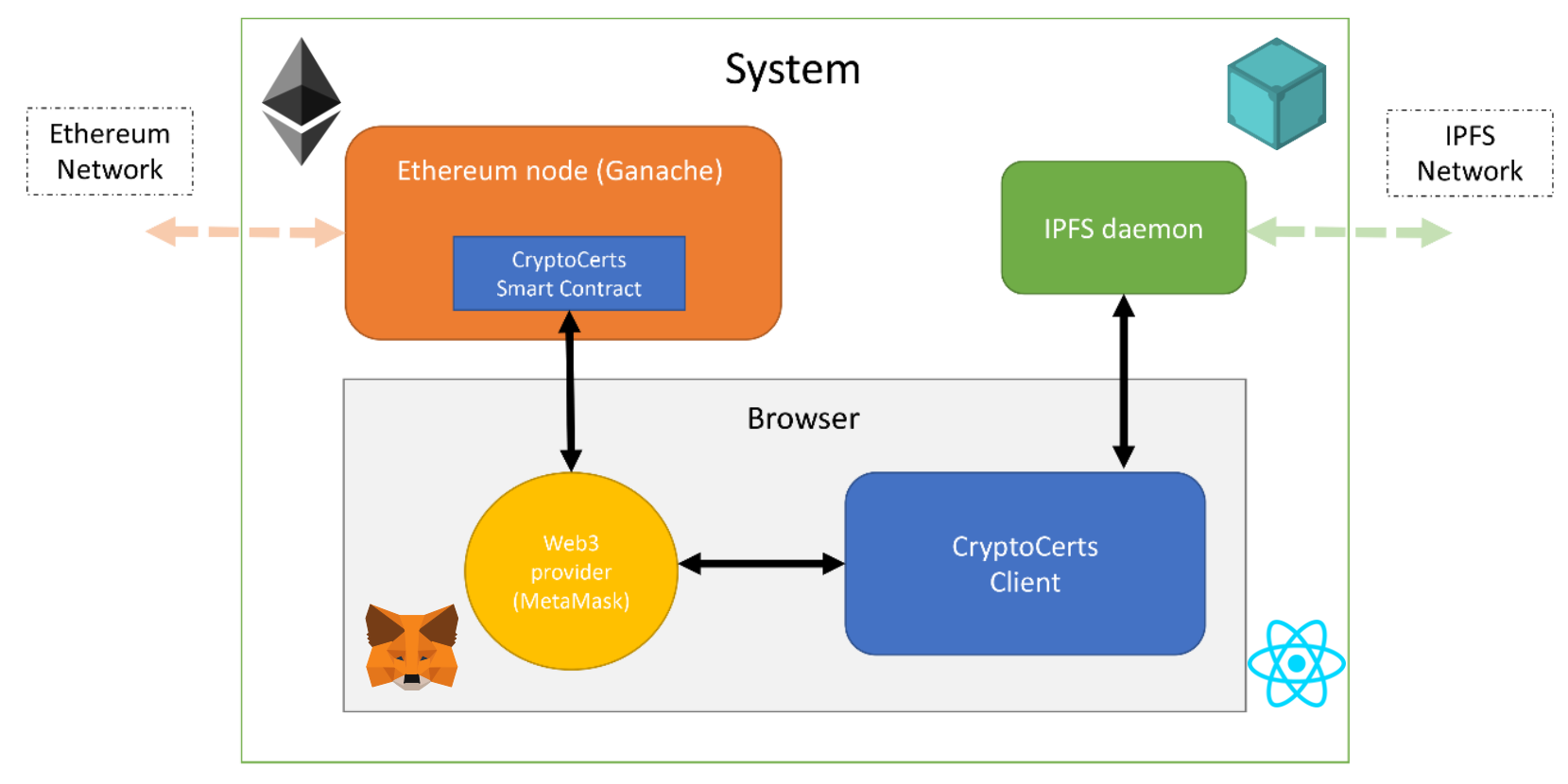
Πηγή: S. Sayeed, H. Marco-Gisbert και T. Caira

# 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



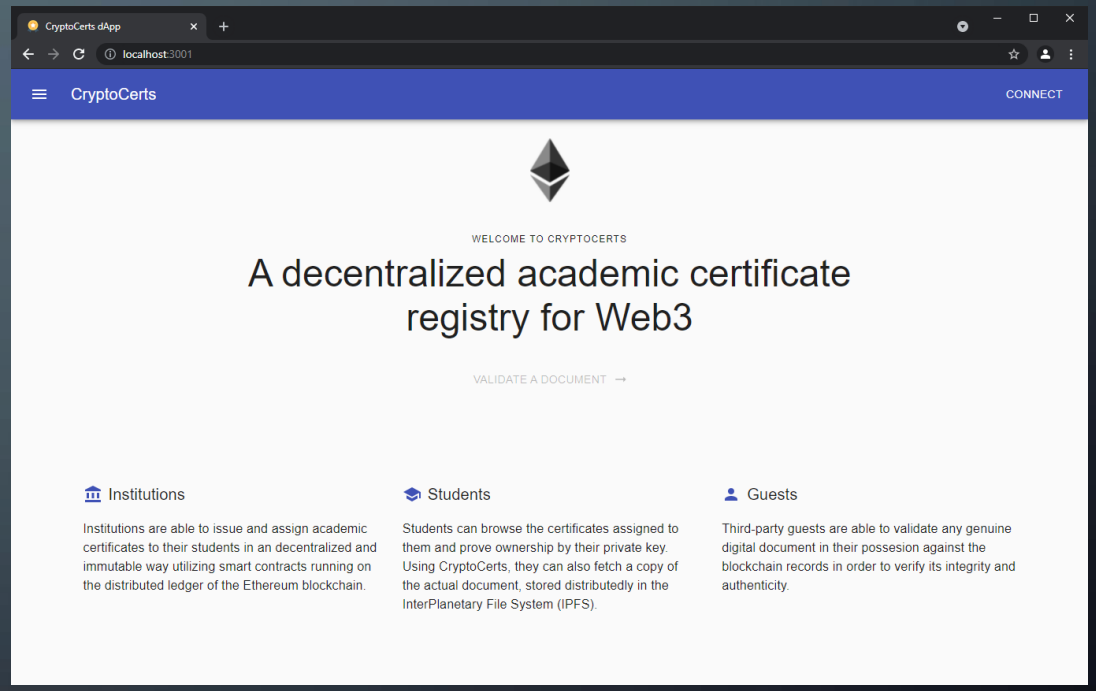

# CRYPTOCERTS – Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ




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

```solidity
// SPDX-License-Identifier: UNLICENSED

pragma solidity ^0.7.0;

import "../node_modules/@openzeppelin/contracts/access/Ownable.sol";

contract InstitutionFactory is Ownable {
    event InstitutionCreated(
        uint256 indexed id,
        string name,
        address indexed addr
    );

    struct Institution {
        string name;
        string location;
        bool isValid;
    }

    mapping(address => uint256) public ownerToInstitution;
    mapping(uint256 => address) public institutionToOwner;

    Institution[] public institutions;

    /**
     * @dev Throws if called by any account who doesn't beloong to an Institution.
     */
    modifier onlyInstitution() {
        require(
            ownerToInstitution[_msgSender()] != 0,
            "Caller is not an institution owner"
        );
        _;
    }
```

```solidity
    function createInstitution(string memory _name, string memory _location, address _address) public onlyOwner {
        institutions.push(Institution(_name, _location, true));

        uint256 id = institutions.length;
        ownerToInstitution[_address] = id;
        institutionToOwner[id] = _address;

        InstitutionCreated(id, _name, _address);
    }

    function editInstitution(uint256 _id, string memory _name, string memory _location) public onlyOwner {
        institutions[_id].name = _name;
        institutions[_id].location = _location;
    }

    function deleteInstitution(uint256 _id) public onlyOwner {
        Institution memory institution = institutions[_id];
        institution.isValid = false;
        ownerToInstitution[institutionToOwner[_id]] = 0;
        institutionToOwner[_id] = address(0);
    }

    function getInstitutionsCount() external view returns (uint256) {
        return institutions.length;
    }
}
```

Παράδειγμα ενός smart contract

# BRACE YOURSELVES…