ΕΘΝΙΚΗ ΣΧΟΛΗ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ
ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΚΕ΄ ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ

ΤΕΛΙΚΗ ΕΡΓΑΣΙΑ

ΤΙΤΛΟΣ

Μελέτη της τεχνολογίας Blockchain και των εφαρμογών της στις ψηφιακές συναλλαγές

ΤΜ. ΕΞΕΙΔΙΚΕΥΣΗΣ: ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ

Επιβλέπων:

Κλεάνθης Νόου

Σπουδαστής:

Αλέξανδρος Αποστολόπουλος

ΑΘΗΝΑ - 2018

Αλέξανδρος Αποστολόπουλος

Μελέτη της τεχνολογίας Blockchain και των εφαρμογών της στις ψηφιακές συναλλαγές

Περίληψη

Οι Τεχνολογίες Επικοινωνιών και Πληροφορικής (ΤΠΕ) αποτελούν έναν από τους σημαντικότερους παράγοντες αλλαγής των επιχειρηματικών και διοικητικών μοντέλων. Ιδιαίτερα κατά την παρούσα συγκυρία, κατά την οποία η Δημόσια Διοίκηση καλείται να ανταποκριθεί σε πολλαπλές προκλήσεις, να αξιοποιήσει κατά το βέλτιστο τρόπο τους διαθέσιμους πόρους της και να παρέχει υψηλής ποιότητας ηλεκτρονικές υπηρεσίες προς τους πολίτες, οφείλει όχι απλά να παρακολουθεί, αλλά να πρωτοπορεί στις σχετικές εξελίξεις. Στο πλαίσιο αυτό, ο στόχος της παρούσας εργασίας είναι διττός. Αφενός, να φέρει τον αναγνώστη σε επαφή με τις βασικότερες πτυχές μιας από τις δημοφιλέστερες τεχνολογίες ΤΠΕ, την τεχνολογία 'blockchain' και αφετέρου, να παρουσιάσει συγκεκριμένες προτάσεις εφαρμογής στη Δημόσια Διοίκηση, σε πεδία όπου αυτή η τεχνολογία μπορεί να έχει θετικό αντίκτυπο.

Η εργασία αποτελείται από εφτά ενότητες. Μετά την εισαγωγή (1η ενότητα), ακολουθεί η περιγραφή της αρχιτεκτονικής της τεχνολογίας (2η ενότητα), όπου αναλύονται τόσο τα συστατικά μέρη της, όσο και οι υπηρεσίες που μπορεί να παρέχει, οι διαφορετικές υλοποιήσεις της, καθώς και οι διάφορες προσεγγίσεις που μπορούν να ακολουθηθούν για την εφαρμογή της από έναν οργανισμό. Στη συνέχεια (3η ενότητα) γίνεται αναφορά στις σχετικές πρωτοβουλίες που έχει αναπτύξει η Ευρωπαϊκή Επιτροπή και γίνεται μια προσπάθεια να ενταχθεί η συγκεκριμένη τεχνολογία στο γενικότερο πλαίσιο της στρατηγικής της ΕΕ για την Ψηφιακή Ενιαία Αγορά. Παράλληλα γίνεται η απαραίτητη αναφορά στο ισχύον θεσμικό πλαίσιο που αφορά την τεχνολογία αυτή, καθώς και στις επιπρόσθετες νομικές πτυχές της, όπως είναι για παράδειγμα η σχέση της με τον Γενικό Κανονισμό για τα Προσωπικά Δεδομένα (ΓΚΠΔ).

Στην επόμενη ενότητα (4η) αποτυπώνεται η προσπάθεια επιχειρησιακής ανάλυσης της συγκεκριμένης τεχνολογίας, η οποία περιλαμβάνει ανάλυση SWOT, ανάλυση Κύκλου Υπερβολής (Hype Cycle) Gartner, αναφορά στους Κρίσιμους Παράγοντες Επιτυχίας (ΚΠΕ) και σχεδιασμό Δέντρου Απόφασης για την επιλογή ή όχι της τεχνολογίας αυτής από έναν οργανισμό. Στη συνέχεια (5η ενότητα) περιγράφονται οι σημαντικότερες σχετικές εφαρμογές που έχουν υλοποιηθεί σε ευρωπαϊκό επίπεδο, καθώς και οι πρωτοβουλίες που έχουν ληφθεί σε εθνικό επίπεδο στην Ελλάδα. Στην επόμενη ενότητα (6η) επιχειρείται η αναλυτική περιγραφή μιας πιθανής πρότασης, για μια εφαρμογή blockchain σε ένα πεδίο της ελληνικής Δημόσιας Διοίκησης και στην τελευταία ενότητα (7η) περιλαμβάνονται τα συμπεράσματα της εργασίας.

Η εργασία βασίζεται σε ποιοτική έρευνα, με μελέτη και επισκόπηση της βιβλιογραφίας και μελέτη περιπτώσεων για την εξαγωγή συμπερασμάτων. Με μια αναδύουσα τεχνολογία,

όπως είναι το blockchain, με σχεδόν καθημερινές ειδήσεις και δημοσιεύσεις στα σχετικά, εξειδικευμένα μέσα ενημέρωσης, η ποιοτική έρευνα ουσιαστικά αντιπροσωπεύει μια ρεαλιστική προσέγγιση επαφής με το θέμα, πόσο μάλλον όταν η επιστημονική έρευνα σε σχέση με την τεχνολογία αυτή βρίσκεται ακόμα σε εμβρυικό στάδιο και οι περιπτώσεις μελέτης βρίσκονται -στη πλειοψηφία τους- σε επίπεδο σχεδιασμού και προτάσεων. Στο πλαίσιο αυτό, σύμφωνα με τις καλές πρακτικές διεξαγωγής έρευνας, έγινε προσπάθεια αξιολόγησης της ποιότητας των διαδικτυακών πηγών, ώστε στη πλειοψηφία των περιπτώσεων, τα δεδομένα τους να συνάδουν με αυτά άλλων ιστοτόπων, να διαθέτουν παραπομπές ή να αποτελούν έργο αναγνωρισμένων συγγραφέων στον χώρο τους.

Λέξεις Κλειδιά: Blockchain, Bitcoin, Ethereum, Hash, Proof of Work (PoW)

Abstract

Communication and Information Technology (ICT) is one of the most important forces in changing business and administrative models. Particularly at the current juncture, when public administration is called upon to respond to multiple challenges, make optimal use of its available resources and provide high quality e-services to its citizens, it owes not just to monitor, but to pioneer relevant developments. In this context, the aim of this paper is twofold. On the one hand, it aims to bring the reader into touch with the key aspects of one of the most popular ICT technologies, the 'blockchain'. On the other hand, it aims to present concrete implementation proposals to the public administration.

The paper consists of seven modules. After the introduction (1st module), the paper deals with the description of the architecture of this technology (2nd module), and analyzes both its components and the services it can provide, its different implementations, as well as the various approaches that can be followed in its implementation by the public administration. Next, (section 3) the paper refers to the relevant initiatives developed by the European Commission. This is followed by an attempt to integrate this technology into the broader context of the EU Digital Single Market strategy. At the same time, reference is made to the existing regulatory framework concerning this technology, as well as to its additional legal aspects, such as its relation to the General Data Protection Regulation (GDPR).

The next section (4th) puts into practice several techniques, such as a SWOT analysis of the blockchain, a Gartner Hype Cycle Analysis, a reference to Critical Success Factors (CSF), and a Decision Tree for adopting this technology by organizations. The following (section 5) describes the most important applications of the technology at European level, as well as the initiatives taken at national (Greece) level. In the following section (6th) the paper discusses a possible proposal for a blockchain application, in a specific field of the Greek public administration and the last section (7th) contains the conclusions of the paper.

The paper is based on qualitative research, which involves study and review of the literature and of specific case studies to reach conclusions. With an emerging technology, such as the blockchain, with almost daily publications in relevant, specialized media, a quality research essentially represents a realistic approach to the subject, especially as scientific research into this technology is still in embryonic stage and the study cases are –mostly- at the theoretical level.

In this context, according to research principles, an attempt has been made to assess the quality of internet resources, so that in most cases, their data is consistent with that of other sites, or it is the work of respectable authors in their field.

Key Words: Blockchain, Bitcoin, Ethereum, Hash, Proof of Work (PoW)

Περιεχόμενα

«Δηλώνω ρητά ότι, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας, δεν παραβιάζει καθ' οιονδήποτε τρόπο πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής.»

Αθήνα, 10/12/2018

Υπογραφή

Πίνακας Εικονογράφησης

Πίνακας Συντμήσεων

ΑΣΕΠ	Ανώτατο Συμβούλιο Επιλογής Προσωπικού
ΒΔ	Βάση Δεδομένων
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
ΓΓΨΠ	Γενική Γραμματεία Ψηφιακής Πολιτικής
ΕΕ	Ευρωπαϊκή Ένωση
ΕΨΣ	Εθνική Ψηφιακή Στρατηγική
ΚΔΚ	Κρυπτογραφία Δημόσιου Κλειδιού
ΜΜΕ	Μικρές και Μεσαίες Επιχειρήσεις
ΤΚΚ	Τεχνολογία Κατανεμημένου Καθολικού
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών
BaaS	Blockchain as a Service
BC	Blockchain
DLT	Distributed Ledger Technology
PoC	Proof of Concept
PoW	Proof of Work
P2P	Peer to Peer

Εισαγωγή

Τις τελευταίες δεκαετίες η ανθρωπότητα έχει κατακλυστεί από τεχνολογικά επιτεύγματα, τα οποία έχουν μετασχηματίσει και συνεχίζουν να μεταβάλλουν τον τρόπο που λειτουργεί καθημερινά. Ιδιαίτερα η ανάπτυξη νέων Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) είναι μια από τις ισχυρότερες δυνάμεις αλλαγής. Ο στόχος της συγκεκριμένης εργασίας είναι να φέρει τον αναγνώστη σε επαφή με τις βασικές διαστάσεις της τεχνολογίας Blockchain (BC), που είναι μια από τις δημοφιλέστερες τεχνολογίες των τελευταίων ετών, καθώς και να σκιαγραφήσει τις περιοχές, στις οποίες μπορεί να χρησιμοποιηθεί αποτελεσματικά, ιδιαίτερα στο χώρο της Δημόσιας Διοίκησης.

Η περιγραφή της συγκεκριμένης τεχνολογίας και των εφαρμογών που καθιστά δυνατές δεν είναι εύκολη. Εν μέρει επειδή είναι σχετικά περίπλοκη και εν μέρει επειδή το πεδίο βρίσκεται σε έντονη ανάπτυξη με συνεχείς αλλαγές, νέες εφαρμογές και νέους δρώντες. Η κυρίαρχη αντίληψη είναι, πάντως, πως η τεχνολογία αυτή είναι επαναστατική, διότι αντιμετωπίζει ορισμένα σημαντικά προβλήματα και κινδύνους που εμφανίστηκαν με την έλευση του Διαδικτύου, όπως είναι η καλλιέργεια της εμπιστοσύνης, η απόδειξη της γνησιότητας και η ασφάλεια.

Στις συνηθισμένες αρχιτεκτονικές πληροφορικής, η απάντηση σε αυτά τα ερωτήματα είναι η υλοποίηση κλειστών συστημάτων σε ισχυρές κεντρικές οντότητες (εταιρείες, κυβερνήσεις, τράπεζες), πίσω από τείχη προστασίας (firewall) και με ειδικές συνδέσεις δικτύου. Σε αντίθεση, το BC επιτρέπει τη δημιουργία εμπιστοσύνης, την εμπέδωση της ασφάλειας και την απόδειξη της γνησιότητας, με την έξυπνη χρήση της Τεχνολογίας Κατανεμημένου Καθολικού (ΤΚΚ), σε συνδυασμό με κρυπτογραφικές τεχνικές και καθαρή επεξεργαστική ισχύ. Όπως θα αναλυθεί στη συνέχεια, η τεχνολογία περιλαμβάνει, μεταξύ άλλων, τη δημιουργία κωδικών επαλήθευσης, δηλαδή ‘ψηφιακών δακτυλικών αποτυπωμάτων’ για κάθε ψηφιακό αρχείο. Αυτά τα ψηφιακά αποτυπώματα αποθηκεύονται μαζί σε ομάδες σε ένα "μπλοκ". Το μπλοκ στη συνέχεια συνδέεται σε μια αλυσίδα με άλλα μπλοκ, όπου το κάθε ένα περιέχει έναν ψηφιακό αποτύπωμα από το προηγούμενο μπλοκ. Ως εκ τούτου, είναι αδύνατο να προστεθούν νέες πληροφορίες σε παλαιότερα μπλοκ στην αλυσίδα, χωρίς να αλλάξουν τα επόμενα. Χάρη σε αυτήν την ικανότητα το BC εξασφαλίζει την ακεραιότητα των δεδομένων και ενισχύει την εμπιστοσύνη, καθώς η παραποίηση καθίσταται σχεδόν αδύνατη.

Με αυτόν τον τρόπο, οι τεχνολογίες γύρω από το Blockchain διαθέτουν τις δυνατότητες να μετασχηματίσουν τον τρόπο οργάνωσης και λειτουργίας της οικονομίας, επαγγελλόμενες

έναν αποκεντρωμένο κόσμο, όπου οι ίδιοι χρήστες της τεχνολογίας θα κατέχουν αυξημένη εξουσία πάνω στα δεδομένα τους, χωρίς να εξαρτώνται από τρίτες οντότητες για την εμπέδωση της εμπιστοσύνης και της ασφάλειας. Παρόλα αυτά, όπως κάθε τεχνολογία, έτσι και η BC έχει τα πλεονεκτήματα και τα μειονεκτήματά της και ασφαλώς δεν αποτελεί λύση για όλα τα προβλήματα και σε κάθε περίπτωση μελέτης. Υπάρχουν περιπτώσεις όπου φαίνεται να αποτελεί την ιδανική λύση και υπάρχουν άλλες, όπου πιο συμβατικές τεχνολογίες αποτελούν ίσως καταλληλότερη επιλογή.

1. Ιστορική αναδρομή

Η πρώτη περιγραφή της τεχνολογίας BC καταγράφεται πρώτη φορά το 1991 από τους Stuart Haber και W. Scott Stornetta, οι οποίοι προσπαθούσαν να βρουν έναν αποτελεσματικό τρόπο διασφάλισης της ακεραιότητας των ψηφιακών αρχείων. Η ιδέα τους ήταν να κάνουν χρήση μιας αλυσίδας κρυπτογραφημένων μπλοκ πληροφοριών. Μερικά χρόνια αργότερα, το 2008, η πρώτη τεχνικά ολοκληρωμένη εφαρμογή BC προδιαγράφηκε από ένα πρόσωπο (ή ομάδα) γνωστό ως Satoshi Nakamoto, τον 'πατέρα' του 'bitcoin'[1]. Ο Nakamoto βελτίωσε τον υφιστάμενο σχεδιασμό των Haber-Stornetta και χρησιμοποιώντας ένα κρυπτογραφικό πρωτόκολλο και την καινοτόμο ιδέα του PoW (Proof Of Work),[2] κατέστησε εφικτό να προστίθενται νέα μπλοκ πληροφοριών στην αλυσίδα, χωρίς να απαιτείται να έχουν ελεγχθεί και επικυρωθεί από μια κεντρική οντότητα (Narayanan, et al., 2016). Η ιδέα του οδήγησε πολύ σύντομα στα κρυπτονομίσματα[3] για τη διενέργεια ηλεκτρονικών πληρωμών, με δημοφιλέστερο όλων το 'bitcoin'. Σήμερα, η συνολική κεφαλαιοποίηση των κρυπτονομισμάτων ξεπερνά τα 100 δις δολάρια[4].

Πλέον, μετά το 2014, το BC βρίσκεται στην έκδοση 2.0 με την εισαγωγή του πρωτοκόλλου του 'Ethereum'[5] (Bheemaiah, 2015). Η βασική καινοτομία του Ethereum είναι ότι οι προδιαγραφές του επιτρέπουν την εκτέλεση κώδικα, ενώ παρέχει τη δυνατότητα ανάπτυξης εφαρμογών, όπως έξυπνα συμβόλαια (Smart Contracts), επιτρέποντας στους προγραμματιστές να δημιουργήσουν αποκεντρωμένες εφαρμογές (Dapps) που εγκαθίστανται στο ίδιο το δίκτυο BC.

Από το 2015, η πιο γνωστή εφαρμογή της τεχνολογίας BC, το κρυπτονόμισμα bitcoin, έχει αρχίσει να λαμβάνει σοβαρή προσοχή από την επιχειρηματική (ιδίως χρηματοπιστωτική) κοινότητα. Έκτοτε και σταδιακά, η τεχνολογία BC εξελίσσεται με γοργούς ρυθμούς, με την εμφάνιση νέων εφαρμογών και την εκτίναξη του ενδιαφέροντος, από επαγγελματίες, μεγάλες εταιρείες και χρηματοπιστωτικούς κολοσσούς. Για παράδειγμα, το 2015-2016 η IBM άνοιξε ένα ερευνητικό κέντρο BC καινοτομίας στη Σιγκαπούρη. (Williams, 2016), η τράπεζα Goldman Sachs δήλωσε ότι το BC μπορεί να αλλάξει τα πάντα (Insider, 2015), οι εταιρείες που δραστηριοποιούνται στο χώρο του BC συνεργάστηκαν και δημιούργησαν το Παγκόσμιο

[1] Ο όρος bitcoin χρησιμοποιείται εδώ για να περιγράψει το πρωτόκολλο που εφαρμόστηκε στο bitcoin.
[2] Μηχανισμός επίτευξης συναίνεσης μεταξύ μηχανών, που θα εξηγηθεί στο επόμενο κεφάλαιο.
[3] Ένα κρυπτονόμισμα είναι ένα κρυπτογραφημένο ψηφιακό νόμισμα. Για αναλυτικότερα, βλ. σελ. 25
[4] Για μια λίστα με την κεφαλαιοποίηση ανά κρυπτονόμισμα βλ. https://coinmarketcap.com/
[5] Για πιο αναλυτικά βλ. σελ. 28

Φόρουμ Blockchain, ενώ 40 διεθνείς χρηματοπιστωτικοί οργανισμοί έχουν ενώσει τις δυνάμεις τους, επενδύοντας πάνω από 200 εκατ. δολάρια για να προσπαθήσουν να αυτοματοποιήσουν την εκτέλεση χρηματοπιστωτικών συναλλαγών μεταξύ τραπεζών μέσω BC (Rizzo, 2016).

Επιπλέον, σε επίπεδο κυβερνήσεων και διεθνών οργανισμών έχουν αρχίσει οι προσπάθειες, αφενός, ανάπτυξης εφαρμογών βασισμένων στη συγκεκριμένη τεχνολογία, αφετέρου, δημιουργίας ενός σχετικού πλαισίου διακυβέρνησης. Η ΕΕ θεωρεί πλέον το BC, μαζί με την Τεχνητή Νοημοσύνη (AI), ως τις δύο περισσότερο υποσχόμενες τεχνολογίες και χρηματοδοτεί σχετικές δράσεις από τα ερευνητικά της προγράμματα (FP7, HORIZON) ήδη από το 2013, ενώ η Ευρωπαϊκή Επιτροπή ανακοίνωσε τον Φεβρουάριο του 2018 τη σύσταση Παρατηρητηρίου και Φόρουμ για το BC, με σκοπό την παρακολούθηση των εξελίξεων και την προώθησή της νέας τεχνολογίας (European Comimssion, 2018).

2. Θεωρητική Τεκμηρίωση

2.1. Το πρόβλημα της διπλής δαπάνης

Ο Satoshi Nakamoto, προδιαγράφοντας το πρωτόκολλο του bitcoin, προσπαθούσε να λύσει το πρόβλημα της 'διπλής δαπάνης'. Η διπλή δαπάνη είναι ένα πιθανό ελάττωμα σε ένα σύστημα ψηφιακών συναλλαγών, στο οποίο το ίδιο ψηφιακό νόμισμα μπορεί να δαπανηθεί περισσότερες από μία φορές. Αυτό είναι εφικτό επειδή ένα ψηφιακό νόμισμα είναι, ουσιαστικά, ένα ψηφιακό αρχείο που μπορεί να αντιγραφεί ή να παραποιηθεί . Όπως και με τα πλαστά χρήματα, αυτές οι διπλές δαπάνες δημιουργούν πληθωρισμό, δημιουργώντας μια ποσότητα νέου νομίσματος που δεν υπήρχε προηγουμένως. Αυτό υποτιμά το νόμισμα σε σχέση με άλλες νομισματικές μονάδες, μειώνει την εμπιστοσύνη των χρηστών και τελικά, υπονομεύει την επιβίωση του νομίσματος.

Συνοπτικά, η μορφή που μπορεί να προσλάβει η πρόληψη της διπλής δαπάνης είναι δύο ειδών: Κεντρική ή αποκεντρωμένη (ή κατανεμημένη). Η κεντρική συνήθως περιλαμβάνει μία κεντρική οντότητα, όπως για παράδειγμα, μία τράπεζα, που έχει την εξουσία και την δυνατότητα να ελέγξει εάν έχει δαπανηθεί ένα ψηφιακό νόμισμα και με αυτόν τον τρόπο εμπεδώνει την εμπιστοσύνη στο σύστημα. Το μειονέκτημα της κεντρικής μεθόδου έγκειται στο ότι αντιπροσωπεύει ένα μοναδικό σημείο αστοχίας (Single Point of Failure), από άποψη διαθεσιμότητας και εμπιστοσύνης. Δηλαδή, αν η κεντρική οντότητα αποτύχει στη λειτουργία της, θα οδηγήσει σε παύση της διαθεσιμότητας όλου του συστήματος, καθώς και σε σοβαρή βλάβη στην αξιοπιστία της. Ο Nakamoto (Nakamoto, 2008) με την δημοσίευσή του πρότεινε ένα αποκεντρωμένο σύστημα για την πρόληψη της διπλής δαπάνης, το οποίο και τελικά εφαρμόστηκε ως συστατικό στοιχείο του κρυπτονομίσματος 'bitcoin'.

2.2. Η εμπιστοσύνη στον κυβερνοχώρο[6]

Το υποκείμενο ερώτημα στο οποίο κλήθηκε να απαντήσει ο Nakamoto είναι, συνεπώς, το πώς διασφαλίζεται η εμπιστοσύνη στον κυβερνοχώρο, χωρίς την ύπαρξη μιας έμπιστης

[6] Με τον όρο κυβερνοχώρος υποδηλώνεται το περιβάλλον που έχει δημιουργηθεί από δίκτυα επικοινωνιών που χρησιμοποιούν ηλεκτρονικούς υπολογιστές.

κεντρικής οντότητας. Η εμπιστοσύνη είναι ουσιαστικά η εκτίμηση του κινδύνου σε μια σχέση, μεταξύ δύο ή περισσότερων μερών. Στον κυβερνοχώρο, όπου ερχόμαστε σε επαφή με πολλές άγνωστες οντότητες, η εμπιστοσύνη βασίζεται σε δύο βασικές αρχές της ασφάλειας:

Α) Την αυθεντικοποίηση, δηλαδή την πιστοποίηση της ταυτότητας των χρηστών.

Β) Την εξουσιοδότηση, δηλαδή την πιστοποίηση της κατοχής των απαραίτητων δικαιωμάτων για τη πρόσβαση σε κάποιον πόρο.

Δεν μπορεί να υπάρξει μια βιώσιμη σχέση μεταξύ των μερών, αν το ένα μέρος δεν εμπιστεύεται το άλλο. Ιδιαίτερα σε μια ολοένα και περισσότερο διεθνοποιημένη και ψηφιοποιημένη οικονομία, η διατήρηση της εμπιστοσύνης καθίσταται βαθμιαία περισσότερο απαιτητική σε χρόνο, πολυπλοκότητα και κόστος (Piscini, et al, 2016). Απέναντι σε αυτή τη πρόκληση, η ιδέα του Nakamoto, δηλαδή το BC, δίνει μια τόσο ιδιοφυή, όσο και απλή λύση. Μία λύση που μεταφέρει την πηγή της εμπιστοσύνης από την κεντρική οντότητα, στην ίδια την τεχνολογία και που εμπεδώνει την εμπιστοσύνη, καταργώντας την εμπιστοσύνη (με την κλασική έννοια) αυτή καθαυτή.

2.3. Αρχιτεκτονικό Μοντέλο

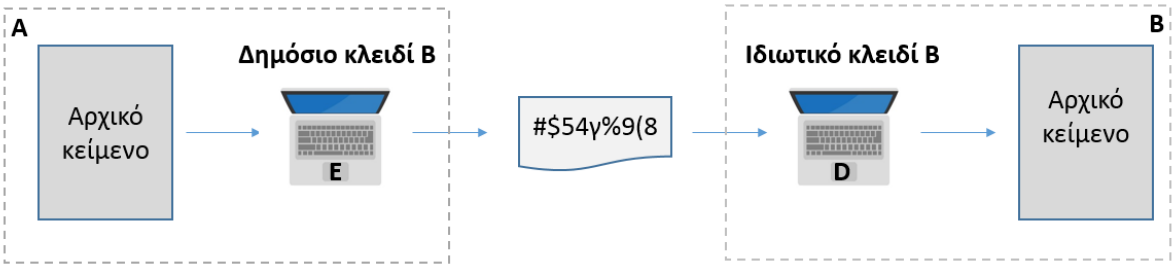
Είναι εφικτό να αποτυπωθεί ένα απλό μοντέλο Blockchain, κάνοντας χρήση μιας αναλογίας του πραγματικού κόσμου. Έστω ότι υπάρχει μια μικρή κοινότητα. Αυτή η κοινότητα έχει μια μικρή οικονομία, με ανθρώπους που αγοράζουν και πωλούν τα εμπορεύματα μεταξύ τους. Κάθε φορά που κάποιος πραγματοποιεί μια συναλλαγή, το αναφέρει στον λογιστή της κοινότητας, ο οποίος την καταγράφει σε ένα κομμάτι χαρτί. Στο τέλος της ημέρας, ο λογιστής πηγαίνει στην πλατεία της κοινότητας και επισυνάπτει δημοσίως το χαρτί με τις συναλλαγές της ημέρας, στο βιβλιάριο ή καθολικό (ledger) με τις συναλλαγές των προηγούμενων ημερών. Επιπλέον, ο λογιστής χρησιμοποιεί βουλοκέρι για να σφραγίσει κάθε επισύναψη, έτσι ώστε κανείς δεν μπορεί να αφαιρέσει ή να παραποιήσει κάποια σελίδα, χωρίς αυτό να γίνει αντιληπτό. Αυτό είναι ένα blockchain σε μια απλή "χάρτινη" εκδοχή. Κάθε σελίδα αντιπροσωπεύει ένα μπλοκ που τοποθετείται σε γραμμική ακολουθία και περιέχει κάποιες συναλλαγές. Και επειδή κάθε επισύναψη είναι σφραγισμένη με βουλοκέρι, ο καθένας μπορεί εύκολα να επιβεβαιώσει ότι κανείς δεν έχει παραποιήσει καμία από τις σελίδες. Με αυτόν τον τρόπο, καθώς το βιβλίο αυτό εκφράζει τις διαχρονικά καταγεγραμμένες και από κοινού

επαληθευμένες συναλλαγές όλης της κοινότητας, αποτελεί ένα ιστορικό, που χαρακτηρίζεται από ακεραιότητα, επαληθευσιμότητα και αυθεντικότητα.

Πράγματι, στην απλούστερη περίπτωση, αυτό είναι ένα BC. Για να γίνει κατανοητό όμως ένα πραγματικό BC θα πρέπει να εμπλουτιστεί αυτή η αναλογία. Συνεπώς, στη συνέχεια ακολουθεί μια προσπάθεια να σκιαγραφηθούν κάποιες βασικές έννοιες και μηχανισμοί που συναθροίζονται, αλληλοεπιδρούν και το συνδιαμορφώνουν.

2.3.1. Κρυπτογραφία Δημόσιου Κλειδιού

Είναι σημαντικό, αρχικά, να γίνει αναφορά στην Κρυπτογραφία Δημόσιου Κλειδιού (ΚΔΚ), καθώς βρίσκεται στον πυρήνα της ασφάλειας των δικτύων BC. Στην κρυπτογραφία δημοσίου κλειδιού ο κάθε χρήστης έχει ένα ζεύγος κλειδιών, ένα ιδιωτικό d, το οποίο το γνωρίζει μόνο ο ίδιος, και δημόσιο e, το οποίο μπορεί να διαθέσει σε όλους τους ενδιαφερόμενους. Τα δύο κλειδιά συνδέονται με μαθηματικό τρόπο έτσι ώστε ένα μήνυμα κρυπτογραφημένο με το ένα κλειδί του ζεύγους να μπορεί να αποκρυπτογραφηθεί μόνο με το άλλο κλειδί του ίδιου ζεύγους. Τυπικά, η κρυπτογράφηση ενός μηνύματος γίνεται με το δημόσιο κλειδί του παραλήπτη ενώ ο παραλήπτης για να αποκρυπτογραφήσει το μήνυμα θα χρησιμοποιήσει το ιδιωτικό του κλειδί (ΕΣΔΔΑ, 2018).



Εικόνα 01: Κρυπτογραφία Δημόσιου Κλειδιού

Η ΚΔΚ είναι ουσιαστικά ο μηχανισμός μέσω του οποίου επιτυγχάνεται η αυθεντικοποίηση των χρηστών και η ασφάλεια των συναλλαγών στο BC, καθώς κάθε συναλλαγή υπογράφεται με το ιδιωτικό κλειδί του αποστολέα και η υπογραφή μπορεί να επαληθευτεί από τον αποδέκτη, με το δημόσιο κλειδί του αποστολέα.

2.3.2. Κρυπτογραφικές Συναρτήσεις Σύνοψης (Hash)

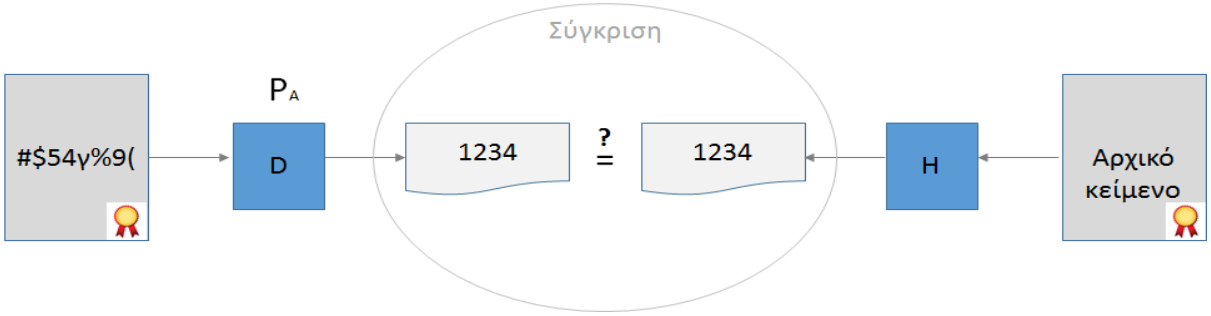
Οι Συναρτήσεις Σύνοψης διαδραματίζουν ιδιαίτερα σημαντικό ρόλο στη σύγχρονη κρυπτογραφία γενικότερα, αλλά και στη λειτουργία του BC ειδικότερα Οι συναρτήσεις αυτές απεικονίζουν στοιχεία ενός συνόλου με πολλά στοιχεία, σε κάποιο άλλο σύνολο με λιγότερα. (Ζάχος, et al., 2015) Ουσιαστικά, με τη χρήση ενός προηγμένου αλγόριθμου, οποιοδήποτε ψηφιακό αρχείο μπορεί να λάβει έναν μοναδικό κωδικό. Ένα παράδειγμα ενός αλγορίθμου που δημιουργεί κρυπτογραφικές συνόψεις (hashes) είναι ο SHA256. Αυτός ο αλγόριθμος λαμβάνει όλα τα ένα και τα μηδενικά που περιγράφουν ένα ψηφιακό αρχείο και τα υπολογίζει εκ νέου, σύμφωνα με ένα καθορισμένο αλλά απρόβλεπτο αποτέλεσμα.[7] Στο τέλος, δημιουργείται μια αλφαριθμητική ακολουθία, δηλαδή μία σύνοψη. Για το ίδιο ψηφιακό αρχείο και τον ίδιο αλγόριθμο κατακερματισμού, το αποτέλεσμα θα είναι πάντα η ίδια σύνοψη και κάθε σύνοψη είναι μοναδική για κάθε ψηφιακό αρχείο, όπως το δακτυλικό αποτύπωμα. Επίσης, δεν είναι δυνατόν –από τη σύνοψη- να ανακατασκευάσουμε το ίδιο το αρχείο που το δημιούργησε. Στη συνέχεια θα αποτυπωθεί σε τι ακριβώς χρησιμεύει η σύνοψη σε ένα δίκτυο BC.

2.3.3. Ψηφιακή Υπογραφή

Σε ασύμμετρα συστήματα κρυπτογράφησης, όπως αποτυπώθηκαν προηγουμένως, οι χρήστες δημιουργούν ένα ζεύγος κλειδιών, το οποίο είναι ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί. Το ιδιωτικό κλειδί προορίζεται να κρατηθεί μυστικό και αξιοποιείται για την ψηφιακή υπογραφή μηνυμάτων που αποστέλλονται σε άλλους χρήστες. Η ψηφιακή υπογραφή σε ένα μήνυμα, πρακτικά, είναι η κρυπτογράφηση της σύνοψης του μηνύματος. Ο υπογράφων θα πρέπει κατά τη διαδικασία δημιουργίας υπογραφής να υπολογίσει τη σύνοψη του μηνύματος και στη συνέχεια να κρυπτογραφήσει αυτή τη σύνοψη με το ιδιωτικό του κλειδί. (ΕΣΔΔΑ, 2018) Για την επαλήθευση της υπογραφής ο παραλήπτης θα χρειαστεί το αρχικό μήνυμα, την υπογραφή και ένα αυθεντικοποιημένο αντίγραφο του δημοσίου κλειδιού του υπογράφοντος. Ο παραλήπτης θα πρέπει να αποκρυπτογραφήσει την υπογραφή χρησιμοποιώντας το δημόσιο

[7] Μια απεικόνιση του πώς λειτουργεί ένας αλγόριθμος σαν τον SHA256 είναι για παράδειγμα ο εξής: Πάρτε κάθε τρίτο ψηφίο στο αρχείο, πολλαπλασιάστε τον αριθμό με 7 και διαιρέστε το σύνολο με κάθε τέταρτο αριθμό στο αρχείο, κατόπιν συνδυάστε κάθε αριθμό που δεν χρησιμοποιείται στο προηγούμενο υπολογισμό στον αριθμό που έχετε, κλπ.

κλειδί του υπογράφοντος, να υπολογίσει εκ νέου τη σύνοψη του μηνύματος από το αρχικό μήνυμα και τελικά, να συγκρίνει τις δύο συνόψεις.



Εικόνα 02: Μηχανισμός Ψηφιακής Υπογραφής

Η δημιουργία ενός ζεύγους κλειδιών είναι ανάλογη με τη δημιουργία ενός λογαριασμού στο BC, καθώς το λογισμικό που δημιουργεί τον λογαριασμό, ουσιαστικά δημιουργεί ένα ιδιωτικό και ένα δημόσιο κλειδί για τον χρήστη, τα οποία συσχετίζονται με τον ανωτέρω μαθηματικό τρόπο. Επίσης, κάθε συναλλαγή που εκτελείται στο BC υπογράφεται ψηφιακά από τον αποστολέα χρησιμοποιώντας το ιδιωτικό κλειδί του. Αυτή η υπογραφή διασφαλίζει ότι μόνο ο κάτοχος του λογαριασμού μπορεί να πραγματοποιήσει συναλλαγές από τον λογαριασμό αυτόν.

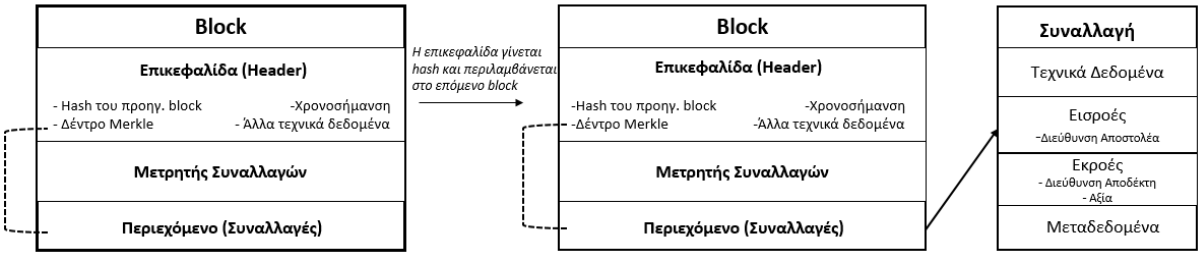
2.3.4. Μπλοκ και Συναλλαγές

Σε ένα μπλοκ καταγράφονται οι πιο πρόσφατες συναλλαγές που έχουν γίνει σε ένα BC δίκτυο. Στο BC του bitcoin αυτές που έχουν γίνει τα τελευταία περίπου 10 λεπτά. Ουσιαστικά, ένα μπλοκ είναι ένα «αποθετήριο δεδομένων», τα οποία, μόλις εγγραφούν, δεν μπορούν να τροποποιηθούν ή να αφαιρεθούν. Τα δεδομένα στα μπλοκ των συναλλαγών περιέχουν συνήθως στοιχεία της συναλλαγής, όπως τί αξία ανταλλάχθηκε, τα μέρη της συναλλαγής, διάφορα μεταδεδομένα σχετικά με τη συναλλαγή, καθώς και τη κρυπτογραφική σύνοψη του προηγούμενου μπλοκ, με το οποίο συνδέεται (Grech & Camilleri, 2017) Η είσοδος της σύνοψης είναι ουσιαστικά όλες οι συναλλαγές που έχουν πραγματοποιηθεί μέχρι εκείνη τη στιγμή και έτσι, η προκύπτουσα σύνοψη εξόδου αντιπροσωπεύει την τρέχουσα κατάσταση του BC[8]. Η σύνοψη εξόδου χρησιμοποιείται στη συνέχεια για να συμφωνηθεί μεταξύ όλων των

[8] Όλη η κατάσταση του blockchain (για παράδειγμα 200 περίπου Gigabyte για το bitcoin), σε μόλις 256bits.

συμμετεχόντων, ότι η κατάσταση είναι μία και μοναδική: Αν κάθε μέλος του δικτύου έχει την ίδια σύνοψη, όλα τα μέρη νιώθουν εμπιστοσύνη στα εγγεγραμμένα στο κοινό βιβλιάριο δεδομένα. (Rabbani, 2017).

Σχηματικά:



Εικόνα 03: Περιεχόμενο ενός μπλοκ και μιας συναλλαγής

Συνεπώς, είναι προφανές ότι η αλλοίωση της αλυσίδας θα απαιτούσε όχι μόνο την αλλαγή μιας συναλλαγής, αλλά την αλλαγή των πληροφοριών όλων των επικεφαλίδων των μπλοκ που δημιουργήθηκαν ύστερα από τη συγκεκριμένη συναλλαγή, κάτι ιδιαίτερα δύσκολο. Το γεγονός αυτό προσδίδει στο BC ένα από τα μεγαλύτερα πλεονεκτήματά του, την αμεταβλητότητα των δεδομένων.

2.3.5. Κόμβοι (nodes)

Ένα τυπικό δίκτυο εξυπηρετητή - πελάτη (server - client) περιλαμβάνει πολλούς υπολογιστές (clients) που συνδέονται με τουλάχιστον έναν κεντρικό διακομιστή (server). Τα περισσότερα δεδομένα και οι εφαρμογές βρίσκονται εγκατεστημένες στο διακομιστή και όταν οι πελάτες χρειάζονται πρόσβαση σε αυτούς τους πόρους, αυτή παρέχεται από τον διακομιστή. Αντιθέτως, το BC στηρίζεται σε ένα δίκτυο P2P (Peer to Peer)[9], όπου ο κάθε κόμβος είναι το θεμέλιο που επιτρέπει στο δίκτυο να λειτουργήσει. Ένας κόμβος μπορεί να είναι οποιαδήποτε ενεργή ηλεκτρονική συσκευή, συμπεριλαμβανομένου ενός υπολογιστή, εφόσον είναι συνδεδεμένος στο διαδίκτυο και ως εκ τούτου έχει διεύθυνση IP.

[9] Ένα δίκτυο υπολογιστών peer-to-peer (ή P2P) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα. Πληροφορίες που βρίσκονται στον ένα κόμβο μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα.

Σε ένα BC, κάθε κόμβος θεωρείται ίσος, ωστόσο ορισμένοι κόμβοι έχουν διαφορετικούς ρόλους στον τρόπο με τον οποίο υποστηρίζουν το δίκτυο. Για παράδειγμα, ένας πλήρης κόμβος (full node) κατέχει ένα πλήρες αντίγραφο του καθολικού, ελέγχει και επαληθεύει όλες τις νέες συναλλαγές, προσθέτει τα επαληθευμένα μπλοκ στο BC και ενημερώνει / επικοινωνεί με τους υπόλοιπους κόμβους. Είναι σημαντικό να επισημανθεί ότι για να εγγραφεί μια συναλλαγή στο BC, πρέπει τα μέρη που εμπλέκονται - και μόνο αυτά - να δηλώσουν τη συναίνεσή τους. Οι υπόλοιποι κόμβοι απλά επιβεβαιώνουν ότι τα συγκεκριμένα μέρη μπορούν να πραγματοποιήσουν τη συναλλαγή[10]. Όταν συμβεί αυτό, η συναλλαγή εγγράφεται στο μπλοκ, αναμένοντας την επεξεργασία και επιβεβαίωση.

Στα δημόσια BC, κάποιοι από τους πλήρεις κόμβους επεξεργάζονται επιπλέον τις συναλλαγές που εισάγονται σε κάθε μπλοκ. Αυτοί οι κόμβοι, καθώς συνεισφέρουν πρόθυμα τους υπολογιστικούς τους πόρους για την επεξεργασία και επικύρωση των συναλλαγών, έχουν την ευκαιρία να εισπράξουν τυχόν τέλη των συναλλαγών και να κερδίσουν μια ανταμοιβή στο εκάστοτε κρυπτονόμισμα του πρωτοκόλλου που εξυπηρετούν. Αυτό είναι γνωστό ως εξόρυξη (mining) και οι κόμβοι αυτοί ως ανθρακωρύχοι (miners). (Lisk Academy, 2018) Στο παράδειγμα του bitcoin, λόγω της αυξανόμενης δυσκολίας του πρωτοκόλλου του, η επεξεργασία αυτών των συναλλαγών απαιτεί -πλέον- τεράστιες ποσότητες επεξεργαστικής ισχύος και ενέργειας.

2.3.6. Μηχανισμός συναίνεσης

Σε ένα δημόσιο BC[11] δεν υπάρχει η έννοια της κεντρικής οντότητας που να δημιουργεί την απαραίτητη εμπιστοσύνη στους συναλλασσόμενους. Έτσι, έπρεπε να βρεθεί ένας άλλος μηχανισμός, που να επιτρέπει να καλλιεργηθεί εμπιστοσύνη.[12] Υπάρχουν διάφοροι τέτοιοι μηχανισμοί, αλλά ο πιο δημοφιλής, τον οποίο εισήγαγε ο Nakamoto, είναι ο 'Proof of Work' (PoW), που εφαρμόζεται στο δημόσιο BC του Bitcoin και -προς το παρόν- και στο Ethereum[13].

Με αυτό το σύστημα όταν συμπληρωθεί ένας αριθμός συναλλαγών, τα δεδομένα τους ενσωματώνονται σε ένα μπλοκ και ένας κρυπτογραφικός γρίφος αποστέλλεται στους κόμβους.

[10] Ουσιαστικά ελέγχουν με τα δημόσια κλειδιά που αντιστοιχούν στις διευθύνσεις των συναλλασσομένων, αν η υπογραφή της συναλλαγής είναι όντως με τα ιδιωτικά τους κλειδιά, ώστε να επιβεβαιώσουν ότι οι συγκεκριμένοι χρήστες διαθέτουν τα εχέγγυα ώστε να προβούν στη συναλλαγή αυτή.

[11] Αυτό δεν ισχύει στα ιδιωτικά blockchain, όπως θα αναλυθεί παρακάτω.

[12] Ένα πρόβλημα που είναι γνωστό ως «Το Πρόβλημα των Βυζαντινών Στρατηγών». Για πιο αναλυτικά βλ. https://en.wikipedia.org/wiki/Byzantine_fault_tolerance#Byzantine_Generals'_Problem

[13] Άλλοι μηχανισμοί είναι ο Proof of Stake, ο Delegated Byzantine Fault Tolerance (dBFT) κλπ.

(Thompson, 2016)). Ο κρυπτογραφικός γρίφος αφορά το αποτέλεσμα της συνάρτησης σύνοψης του συγκεκριμένου μπλοκ, το οποίο για να είναι έγκυρο θα πρέπει να έχει συγκεκριμένη μορφή, με ένα συγκεκριμένο πλήθος αρχικών μηδενικών. (Ζάχος, et al., 2015). Αυτό κάνει τον υπολογισμό του εξαιρετικά δύσκολο και χρονοβόρο, εάν βέβαια η συνάρτηση σύνοψης έχει τις επιθυμητές ιδιότητες τυχαιότητας. Οι κόμβοι - miners ανταγωνίζονται για την επίλυση του κρυπτογραφικού γρίφου, του οποίου η επίλυση αποφέρει ένα ορισμένο κέρδος (προς το παρόν 12.5 bitcoins). Ο πρώτος miner που θα λύσει τον γρίφο, εκπέμπει τη λύση (μαζί με το συγκεκριμένο μπλοκ με τις συναλλαγές) στο δίκτυο των κόμβων που τηρούν το κοινό καθολικό και λαμβάνει την σχετική αμοιβή. Το δίκτυο των κόμβων επαληθεύει τη λύση,[14] προσθέτει το μπλοκ στην αλυσίδα και ενημερώνει το καθολικό. Με τον τρόπο αυτό δημιουργείται η αλυσίδα των μπλοκ με τις συναλλαγές, η οποία διαρκώς επεκτείνεται.[15] (Drescher, 2017)

2.3.7. Πορτοφόλι (‘wallet’)

Για να αποκτήσει κάποιος πρόσβαση στο BC και να πραγματοποιήσει συναλλαγές, απαιτείται να εγκαταστήσει στην τοπική του συσκευή μια εφαρμογή λογισμικού (client)[16], η οποία είναι απαραίτητη για τη διαμεσολάβηση μεταξύ του χρήστη και του δικτύου. Η εφαρμογή λογισμικού, που ονομάζεται συνήθως «πορτοφόλι» (wallet), μπορεί είτε να εγκατασταθεί απευθείας σε μια συσκευή, είτε να εκτελεστεί μέσω ενός προγράμματος περιήγησης ιστού (web browser) και μπορεί να χρησιμοποιηθεί τόσο για την αποστολή, όσο και για τη λήψη ψηφιακών στοιχείων στο BC.

Τα περισσότερα πορτοφόλια στηρίζουν τη λειτουργία τους σε τρεις βασικές πληροφορίες: μια διεύθυνση, που χρησιμοποιείται για την αποστολή και τη λήψη κρυπτονομισμάτων (ή γενικότερα, κάποιου ψηφιακού στοιχείου) και το αντίστοιχο δημόσιο και ιδιωτικό κλειδί της διεύθυνσης αυτής. Το πορτοφόλι, δηλαδή, αποδίδει μια δημόσια διεύθυνση στον χρήστη και δημιουργεί αυτόματα ένα ιδιωτικό κλειδί, με το οποίο αυτή συνδέεται με κρυπτογραφικό τρόπο. Όταν πραγματοποιείται μια συναλλαγή από ένα πορτοφόλι, το λογισμικό υπογράφει τη συναλλαγή με το ιδιωτικό κλειδί του χρήστη και με τον

[14] Ενώ η λύση του γρίφου από τους miners απαιτεί τεράστια υπολογιστική ισχύ, η επαλήθευση της λύσης από τους κόμβους είναι πολύ απλή.

[15] Ενδεικτικά, στην πλατφόρμα blockchain του bitcoin, ένα μπλοκ προστίθεται κάθε 12 λεπτά.

[16] Υπάρχουν πολλά σχετικά λογισμικά. Για παράδειγμα ο ‘Parity Ethereum’ και ο ‘Geth Ethereum’ είναι οι πιο δημοφιλείς Ethereum clients.

τρόπο αυτό αποδεικνύει σε ολόκληρο το δίκτυο ότι διαθέτει τα εχέγγυα για να προβεί σε αυτή. (Blockchain Support, 2018). Κάθε μέρος της συναλλαγής, καθώς και συνολικά το δίκτυο, μπορεί να δει την συναλλαγή και να εξακριβώσει σε ποιόν ανήκουν τα περιουσιακά στοιχεία, χωρίς όμως να γνωρίζει τις ταυτότητες των συγκεκριμένων χρηστών.

Ορισμένα πορτοφόλια λαμβάνουν στη συσκευή του χρήστη το πλήρες αρχείο του BC, το οποίο δίνει στους χρήστες τους τη δυνατότητα εγγραφής, αποθήκευσης και συγχρονισμού του κοινού καθολικού και τους καθιστά πλήρεις κόμβους. Κάποια άλλα πορτοφόλια, ιδιαίτερα αυτά που απευθύνονται σε κινητές συσκευές (mobile wallets), οι οποίες δεν έχουν επαρκή μνήμη και επεξεργαστική ισχύ για το πλήρες αρχείο του BC, είναι γνωστά ως 'light clients'. Αυτά τα πορτοφόλια δεν αλληλοεπιδρούν άμεσα με το ίδιο το BC, αλλά απαιτείται να συνδεθούν πρώτα με κάποιον πλήρη κόμβο. (Sardan, 2018)

2.3.8. Κρυπτονομίσματα ή tokens

Σχεδόν κάθε πρωτόκολλο δημόσιου BC προβλέπει την δημιουργία κρυπτονομισμάτων, τα οποία είναι απαραίτητα για τη συμμετοχή στην εκάστοτε πλατφόρμα. Τα κρυπτονομίσματα είναι κρυπτογραφημένα ψηφιακά νομίσματα και μπορεί να είναι είτε Altcoins[17], είτε Tokens (Aziz, 2018). Η πρώτη κατηγορία, με την εξαίρεση του Ether του BC Ethereum, είναι κρυπτονομίσματα που έχουν στηριχθεί στον βασικό κώδικα του bitcoin, τον οποίο έχουν τροποποιήσει. Αντιθέτως, τα tokens απεικονίζουν ψηφιακά κάποιο εμπορεύσιμο περιουσιακό στοιχείο και είναι πολύ πιο εύκολο να δημιουργηθούν (υπάρχουν έτοιμα πρότυπα), χωρίς να απαιτείται η τροποποίηση του κώδικα του εκάστοτε πρωτοκόλλου. Η αξία των κρυπτονομισμάτων υπάρχει μόνο μέσα στο οικοσύστημα λειτουργίας ενός συγκεκριμένου πρωτοκόλλου και καθορίζεται από τα τεχνικά χαρακτηριστικά του πρωτοκόλλου, τις λειτουργικές του δυνατότητες και φυσικά, την απήχησή και τη διάδοσή του στην κοινότητα στην οποία απευθύνεται. (Λογαράς, 2018)

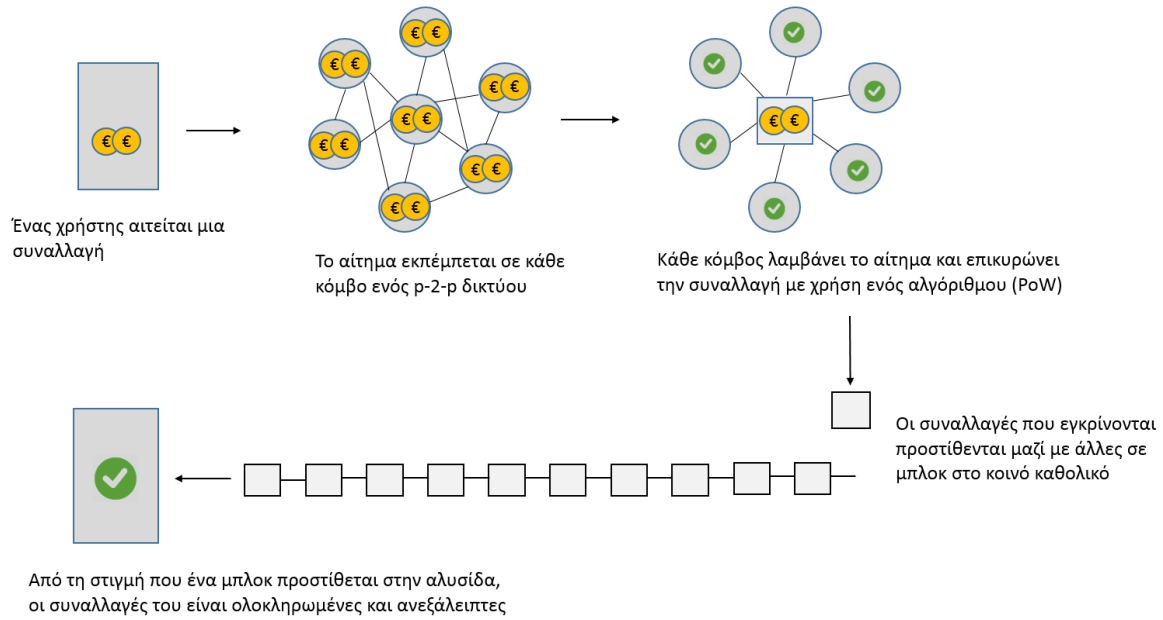
2.3.9 Συνοψίζοντας

Συμπερασματικά, το blockchain συνδυάζει με εκπληκτικά ευφυή τρόπο όλες τις θεμελιώδεις κρυπτογραφικές τεχνικές, όπως οι ψηφιακές υπογραφές, οι συναρτήσεις σύνοψης

[17] Alternative Cryptocurrency Coins

κ.α., προκειμένου να επιτρέψει στους χρήστες του να συναλλάσσουν ψηφιακά στοιχεία με ασφάλεια, χωρίς κεντρικό έλεγχο. Το BC είναι στην ουσία ένα κοινό βιβλιάριο ή καθολικό στο οποίο αποθηκεύονται κι επαληθεύονται πληροφορίες και δεδομένα. Η θεμελιώδης διαφορά από τα υφιστάμενα μητρώα και βάσεις δεδομένων (ΒΔ) είναι ότι, για την τήρησή του δεν είναι αρμόδια μία κεντρική αρχή, αλλά οι λεγόμενοι κόμβοι, δηλαδή χρήστες οι οποίοι, έχοντας εγκαταστήσει το απαιτούμενο λογισμικό (πορτοφόλι), επεξεργάζονται και εγκρίνουν τις συναλλαγές και ενημερώνουν το κοινό καθολικό για οποιαδήποτε αλλαγή, ώστε ανά πάσα στιγμή, όλοι να κατέχουν την ίδια ακριβώς εκδοχή.[18] Τα δεδομένα επαληθεύονται και εντάσσονται στα μπλοκ με τη χρήση κρυπτογραφικών μεθόδων, με τέτοιο τρόπο ώστε να δημιουργείται μία συνεχής αλυσίδα δεδομένων, της οποίας κανένας κρίκος δεν μπορεί να παραποιηθεί, χωρίς να επηρεαστούν αναπόφευκτα όλες οι μεταγενέστερες καταχωρήσεις. (Ζάχος, et al., 2015)

Σχηματικά:



Εικόνα 04: Μηχανισμός του Blockchain

[18] Η έκδοση που 'τρέχει' στην πλειοψηφία των υπολογιστών θεωρείται ότι είναι η «πραγματική» έκδοση, οπότε ο μόνος τρόπος να παραποιηθεί το καθολικό, θα ήταν η κακόβουλη συνεργασία της πλειοψηφίας των κόμβων. Για αναλυτικότερα βλ. σελ. 48 (Επίθεση 51%)

Συνεπώς, συνοπτικά, τα βασικά χαρακτηριστικά του BC είναι τα εξής:

- Είναι μια αποκεντρωμένη ΒΔ που βασίζεται σε ένα δίκτυο P2P.
- Επιτρέπει στους χρήστες του να συναλλάσσουν ψηφιακά στοιχεία με τη βοήθεια ενός κατανεμημένου βιβλιαρίου συναλλαγών, το οποίο κατέχουν οι ίδιοι.
- Τα δεδομένα του βιβλιαρίου χαρακτηρίζονται από αμεταβλητότητα.
- Παρέχει διαφάνεια των συναλλαγών, σε συνδυασμό με ανωνυμοποίηση των χρηστών.
- Λειτουργεί με αυτοματοποιημένη λογική (υπολογιστική) μεταξύ μηχανών.

2.4. Blockchain – Εκδόσεις

2.4.1. Blockchain v1.0 (Bitcoin)

Η αρχική εφαρμογή της τεχνολογίας BC οδήγησε στην πρώτη (v1.0) εφαρμογή της: τα κρυπτονομίσματα (με πρώτο και πιο γνωστό το bitcoin), για την διενέργεια χρηματικών συναλλαγών στο διαδίκτυο. Άλλωστε αυτός ήταν και ο αρχικός στόχος της τεχνολογίας, καθώς σύμφωνα με τον Nakamoto, αυτό που προσπαθούσε να πετύχει ήταν η δημιουργία ενός ηλεκτρονικού συστήματος πληρωμών, βασισμένου όχι στην εμπιστοσύνη, αλλά στη κρυπτογραφική επαλήθευση. Έτσι, στην πρώτη του έκδοση το BC παρέχει στους συμμετέχοντες στο δίκτυο ένα σύνολο προκαθορισμένων λειτουργιών, που σχετίζονται με την Απόδειξη της Ιδιοκτησίας (Proof of Ownership). Σε αυτή τη περίπτωση, το BC χρησιμοποιείται -σε συνδυασμό με την εξουσιοδότηση και την αυθεντικοποίηση- για να αποδείξει την ιδιοκτησία σε ένα περιουσιακό στοιχείο. (Swan, 2018).

Παρόλα αυτά, η τεχνολογία BC, λόγω των εγγενών χαρακτηριστικών της, παρουσιάζει πλεονεκτήματα που μπορούν να χρησιμοποιηθούν και σε άλλες εφαρμογές, μεταξύ των οποίων αναφέρονται ενδεικτικά: (Drescher, 2017)

- **Απόδειξη της Ύπαρξης (Proof of Existence)**

Εδώ η αποθήκευση των δεδομένων έχει κύριο στόχο την απόδειξη της ύπαρξης. Για παράδειγμα, μητρώα με ονόματα, πατέντες, άδειες κλπ.

- **Απόδειξη του Χρόνου Proof of time)**

Σε αυτή τη περίπτωση είναι σημαντική και η απόδειξη της χρονικής στιγμής, στη οποία προστέθηκε η εγγραφή στο BC. Αυτό καθίσταται δυνατό λόγω της εγγενούς δυνατότητάς του BC να εγγράφει τον χρόνο σε κάθε μπλοκ, όταν εισάγεται στο δίκτυο.

- **Απόδειξη της Σειράς (Proof of order)**

Λόγω της προηγούμενης δυνατότητας, ουσιαστικά το BC προσφέρεται για την απόδειξη της αλληλουχίας των γεγονότων. Περιπτώσεις που μπορούν να ωφεληθούν από αυτό το χαρακτηριστικό είναι αυτές για τις οποίες έχει σημασία η χρονική σειρά των γεγονότων, όπως για παράδειγμα η παρακολούθηση μιας διαδικασίας δημόσιων προμηθειών, μιας διαδικασίας αιτήσεων κ.α

2.4.2. Blockchain v2.0 (Ethereum)

Η νέα γενιά blockchain (v2.0) είναι αυτή που επιτρέπει τα λεγόμενα έξυπνα συμβόλαια, (Smart Contracts), δηλαδή μικρά προγράμματα λογισμικού που εκτελούνται μέσα στο BC. Το πιο διακεκριμένο BC 2.0 είναι αυτό του Ethereum, που δόθηκε στη δημοσιότητα στις 30 Ιουλίου 2015 από τον Vitalik Buterin (Buterin, 2015).

Όπως και στην περίπτωση του Bitcoin, το Ethereum δεν ελέγχεται από κάποια κεντρική αρχή, αλλά είναι μια πλατφόρμα ανοιχτού κώδικα. Κάθε μπλοκ διατηρείται και ενημερώνεται από πολλούς κόμβους, που είναι συνδεδεμένοι στο δίκτυο. Στην καρδιά του Ethereum βρίσκεται η εικονική μηχανή Ethereum Virtual Machine, (EVM), η οποία μπορεί να εκτελέσει κώδικα οποιασδήποτε αλγοριθμικής πολυπλοκότητας. Κάθε κόμβος του δικτύου χρησιμοποιεί την EVM και εκτελεί ακριβώς τις ίδιες οδηγίες με τους υπόλοιπους κόμβους (Buntinx, 2017). Ο μηχανισμός που χρησιμοποιείται για την επικύρωση των καινούργιων μπλοκ είναι προς το παρόν ο Proof-of-Work. Δηλαδή, και σε αυτή τη περίπτωση το κίνητρο των miners για την παροχή της επεξεργαστικής τους ισχύος και την εξόρυξη των μπλοκ είναι οικονομικό, όμως όχι σε bitcoin, αλλά στο λεγόμενο “gas”, του οποίου η αξία είναι εκφρασμένη σε ‘ether’. Η συνολική κατάσταση του Ethereum BC αντιπροσωπεύει την κατάσταση όλων των ‘έξυπνων συμβολαίων’, όσον αφορά τις εισόδους τους, τις μεταβλητές τους και τις εξόδους τους.

Ένα έξυπνο συμβόλαιο είναι ένα κομμάτι κώδικα που αποθηκεύεται σε ηλεκτρονικό υπολογιστή χωρίς να μπορεί κάποιος να το παραβιάσει. (Κύπρος, 2018) Ο κώδικας εκτελείται όταν μια συναλλαγή αποστέλλεται σε μια διεύθυνση και εκτελεί αυτόματα κάποιες μεθόδους, υπό προκαθορισμένες συνθήκες. Είναι συνεπώς δυνατόν να συμπεριληφθεί ένας κώδικας, που να επιτρέπει την ενσωμάτωση στην συναλλαγή μιας ενέργειας τύπου "εάν X, τότε Y", όπου θα ελέγχει για συγκεκριμένους όρους που πρέπει να πληρούνται ώστε να ενεργήσει αναλόγως. Για παράδειγμα, μπορούμε να φανταστούμε προϊόντα που όταν παραδίδονται στην μεταφορική εταιρεία και σαρώνεται ηλεκτρονικά το barcode τους από τον οδηγό, διενεργείται αυτόματα πληρωμή στο εργοστάσιο παραγωγής κ.α.

Με τα έξυπνα συμβόλαια κατοχυρώνεται η εμπιστοσύνη, καθώς δημιουργείται η βεβαιότητα ότι η συναλλαγή θα εκτυλιχθεί όπως είχε αρχικά συμφωνηθεί. (Gray & Hajduk, 2017) Ταυτόχρονα, ελαττώνεται δραστικά ο κίνδυνος του ανθρώπινου λάθους που εμφιλοχωρεί στα "γραπτά" συμβόλαια και διαδικασίες, καθώς και το κόστος, εφόσον εξαλείφονται οι διαμεσολαβητές.

2.4.3. Blockchain v3.0 (DApps)

Με τα έξυπνα συμβόλαια, τα οποία αποτελούν την βασική 'Κλάση' στην δικιά του, αντικειμενοστραφούς γλώσσα προγραμματισμού (Solidity), το Ethereum επιτρέπει στους χρήστες του να δημιουργούν τις δικές τους λειτουργίες. Με τον τρόπο αυτό, χρησιμεύει ως πλατφόρμα για πολλούς διαφορετικούς τύπους αποκεντρωμένων εφαρμογών (Dapp's) Blockchain, οι οποίες εκτελούν τον κώδικά τους στο δίκτυο του blockchain, χρησιμοποιώντας αποκεντρωμένη αποθήκευση και αποκεντρωμένη επικοινωνία.[19]Η ανάπτυξη των αποκεντρωμένων εφαρμογών στο Ethereum θεωρείται από πολλούς ως το blockchain v3.0.

2.4.4. Μελλοντικά

Σε ότι αφορά το μέλλον (blockchain v4.0), οι περισσότεροι ειδικοί θεωρούν ότι αυτό θα αναφέρεται σε υψηλού επιπέδου ικανοποίηση των επιχειρησιακών απαιτήσεων των οργανισμών και των επιχειρήσεων με λύσεις BC. Για παράδειγμα, οραματίζονται ένα μέλλον

[19] Για μια λίστα με αποκεντρωμένες εφαρμογές της πλατφόρμας του ethereum βλ. https://media.consensys.net/get-to-know-the-47-projects-that-make-up-the-consensys-mesh-478b7d3028c1

όπου τα μηχανήματα θα παραγγέλνουν τα ίδια τους τα ανταλλακτικά, όπου η διαχείριση της εφοδιαστικής αλυσίδας θα γίνεται αυτοματοποιημένα, όπου οι χρηματοοικονομικές συναλλαγές και οι πληρωμές, η συλλογή δεδομένων Internet of Things (IoT), κλπ. θα υλοποιείται με την τεχνολογία BC και με αποκεντρωμένες εφαρμογές. (Unibright, 2017)

2.5. Τεχνικές Υλοποιήσεις

Είναι απαραίτητο να διαχωρίσουμε τις διαφορετικές τεχνικές υλοποιήσεις της τεχνολογίας blockchain, διότι αν και εμφανίζουν κάποιες ομοιότητες, έχουν πολλές διαφορές και παρουσιάζουν διαφορετικά πλεονεκτήματα και μειονεκτήματα. Συνεπώς, η κάθε μία αποτελεί την βέλτιστη λύση σε διαφορετικές συνθήκες/ανάγκες και είναι σκόπιμο να προηγηθεί μια μικρή σχετική ανάλυση.

Ανεξαρτήτως υλοποίησης, όλα τα BC παραμένουν αποκεντρωμένα δίκτυα P2P, όπου κάθε συμμετέχων διατηρεί ένα αντίγραφο ενός κοινόχρηστου καθολικού ψηφιακά υπογεγραμμένων συναλλαγών. Επίσης, σε όλες τις εκδοχές τους διατηρούν συγχρονισμένα τα αντίγραφα του καθολικού, μέσω κάποιου μηχανισμού συναίνεσης, ενώ τέλος, όλα παρέχουν κάποιες εγγυήσεις για την ακεραιότητα του καθολικού. (Jayachandran, 2017) Εκτός από αυτές τις ομοιότητες όμως, παρουσιάζουν σημαντικές διαφορές:

2.5.1. Δημόσιο Blockchain

Η βασική διάκριση μεταξύ δημόσιου και ιδιωτικού BC σχετίζεται με το ποιός μπορεί να συμμετάσχει στο δίκτυο, να εκτελέσει το πρωτόκολλο συναίνεσης και να διατηρήσει το κοινό καθολικό. Ένα δημόσιο δίκτυο BC (π.χ Bitcoin, Ethereum) είναι εντελώς ανοιχτό και ο καθένας μπορεί να συμμετάσχει. Δηλαδή, οποιοσδήποτε μπορεί να εγκαταστήσει το κατάλληλο πορτοφόλι και να ξεκινήσει έναν δημόσιο κόμβο στον τοπικό, ηλεκτρονικό του υπολογιστή, επικυρώνοντας τις συναλλαγές στο δίκτυο και συμμετέχοντας με αυτόν τον τρόπο στη διαδικασία συναίνεσης για τον προσδιορισμό των μπλοκ που προστίθενται στην αλυσίδα. Οποιοσδήποτε, επίσης, μπορεί να στείλει συναλλαγές μέσω του δικτύου και αυτές να συμπεριληφθούν στο BC (αν είναι έγκυρες). Επιπλέον, ο καθένας μπορεί να έχει πρόσβαση σε όλες τις συναλλαγές. Τέλος, το δημόσιο δίκτυο έχει συνήθως έναν μηχανισμό παροχής κινήτρων, που στηρίζεται συνήθως σε κάποιο κρυπτονόμισμα, τόσο για να ενθαρρύνει τους

miners, όσο και για να ενθαρρύνει περισσότερους συμμετέχοντες να ενταχθούν στο δίκτυο. (Blockchain Hub, 2016)

2.5.2. Ιδιωτικό και Κοινοπρακτικό Blockchain

Αντιθέτως, στα ιδιωτικά δίκτυα απαιτείται πρόσκληση για συμμετοχή και οι κανόνες τίθενται από αυτούς που προσκαλούν. Ο μηχανισμός ελέγχου της πρόσβασης μπορεί να ποικίλει. Για παράδειγμα, οι υπάρχοντες συμμετέχοντες θα μπορούσαν να αποφασίζουν για τους μελλοντικούς, ή μια ρυθμιστική αρχή θα μπορούσε να εκδίδει άδειες συμμετοχής. (Jayachandran, 2017) Σε αυτά τα δίκτυα ο υπεύθυνος επικύρωσης των συναλλαγών δεν είναι ο οποιοσδήποτε με πρόσβαση στο διαδίκτυο, αλλά αποκλειστικά ένας οργανισμός[20]ή ένα προεπιλεγμένο σύνολο οργανισμών/κόμβων, από το σύνολο που συμμετέχει[21]. Ένα τέτοιο δίκτυο μπορεί να αξιοποιηθεί, είτε για να συναλλάσσονται αποκλειστικά τα συμμετέχοντα μέρη μεταξύ τους, είτε για να συναλλάσσονται όλοι όσοι ενδιαφέρονται (ανοιχτό), αλλά μόνο κάποιοι προεπιλεγμένοι κόμβοι θα μπορούν να αλλάζουν τους κανόνες και να επαληθεύουν τις συναλλαγές. Σε αυτή τη περίπτωση, οι συμμετέχοντες στο δίκτυο που επικυρώνουν τις συναλλαγές είναι γνωστοί και η εμπιστοσύνη δεν παρέχεται από κάποιο μηχανισμό συναίνεσης -μεταξύ μηχανών-, αλλά από διμερείς ή πολυμερείς νομικές συμφωνίες. Η διαφορά του ιδιωτικού με το κοινοπρακτικό είναι ότι στο κοινοπρακτικό, όλα τα μέρη που καλούνται και συμμετέχουν έχουν ίσα δικαιώματα ψήφου στην διαδικασία συναίνεσης. Και στις δύο περιπτώσεις, πάντως, τα δικαιώματα ανάγνωσης ενδέχεται να είναι δημόσια ή περιορισμένα, ανάλογα με τη περίπτωση και με το αν είναι επιθυμητός ο δημόσιος έλεγχος. (Blockchain Hub, 2016).

Σε ένα τέτοιο πλαίσιο τυπικά δεν υφίσταται η ανάγκη για κάποιο κρυπτονόμισμα, ούτε για κάποιο κίνητρο για να ενεργοποιηθούν τα μέλη να συμμετέχουν. Τα μέλη συμμετέχουν γιατί ανήκουν στους άμεσα ενδιαφερόμενους και αποκομίζουν οφέλη στην γενικότερη επιχειρησιακή λειτουργία τους, όπως μειωμένο κόστος, ευκολία κ.α. Τα βασικά σημεία της ανωτέρω ανάλυσης μπορούν να απεικονιστούν στον ακόλουθο πίνακα:

[20] Για παράδειγμα MONAX, Multichain

[21] Για παράδειγμα, σε μια κοινοπραξία 15 χρηματοπιστωτικών ιδρυμάτων, καθένα από τα οποία λειτουργεί έναν κόμβο, μπορεί να απαιτείται από τα 10 να επικυρώσουν ένα μπλοκ προκειμένου να είναι έγκυρο.
Παραδείγματα: R3 (τράπεζες), EWF (Ενέργεια), B3i (Ασφάλιση)

	Δημόσιο	Ιδιωτικό / Κοινοπρακτικό
Πρόσβαση	*Ελεύθερη*	*Με άδεια*
Ασφάλεια	*Μέσω μηχανισμού συναίνεσης*	*Μέσω προέγκρισης συμμετέχοντων*
Ταυτότητα χρηστών	*Ανώνυμοι/Ψευδωνυμοποιημένοι*	*Γνωστή ταυτότητα/έμπιστοι*
Μηχανισμός συναίνεσης	*Proof of Work κ.α. Μεγάλη κατανάλωση ενέργειας και ευάλωτο στην επίθεση 51%*	*Αλγόριθμος συναίνεσης μόνο μεταξύ των μερών. Πιο "ελαφρύ", γρήγορο και με μικρή κατανάλωση ενέργειας*
Χρόνος ολοκλήρωσης συναλλαγών	*Μεγάλος (όπως του bitcoin, 10 λεπτά)*	*Σε msec*

Εικόνα 05: Σημαντικότερα χαρακτηριστικά Δημόσιου και Ιδιωτικού BC

2.5.3. Πλεονεκτήματα και μειονεκτήματα κάθε υλοποίησης

Αν και τα πλεονεκτήματα και μειονεκτήματα της τεχνολογίας BC -γενικότερα- αναλύονται διεξοδικά σε επόμενο κεφάλαιο, είναι θεμιτό να αναφερθούν εδώ κάποια σημεία που διαφοροποιούν ένα δημόσιο από ένα ιδιωτικό BC:

- Δημόσιο BC

Τα ιδιαίτερα πλεονεκτήματα των δημόσιων BC γενικά εμπίπτουν σε δύο μεγάλες κατηγορίες. Καταρχάς, παρέχουν έναν τρόπο προστασίας των χρηστών από τους παρόχους μιας ηλεκτρονικής υπηρεσίας, καθώς σε ένα δημόσιο BC υπάρχουν ορισμένες ενέργειες που ούτε οι πάροχοι μιας υπηρεσίας δεν έχουν την εξουσία να εκτελέσουν. Αυτό, μπορεί να μην αποτελεί τελικά μειονέκτημα για τους παρόχους, διότι εάν αυτοί καταστήσουν πιο δύσκολες ή και αδύνατες για τους ίδιους κάποιες ενέργειες, τότε οι δυνητικοί χρήστες είναι πιθανότερο να επιδείξουν εμπιστοσύνη και να αλληλοεπιδράσουν με την συγκεκριμένη υπηρεσία. (Buterin, 2015) Δεύτερον, τα δημόσια blockchain είναι εντελώς ανοιχτά, επομένως είναι πιθανό να χρησιμοποιηθούν από πάρα πολλές οντότητες από διαφορετικούς τομείς και με αυτόν τον τρόπο να δημιουργηθούν εξωτερικότητες δικτύου. Για παράδειγμα, για να λειτουργήσει αποτελεσματικά μια υπηρεσία που προϋποθέτει δεδομένα από εντελώς διαφορετικούς τομείς, θα πρέπει αυτά να βρίσκονται στην ίδια βάση δεδομένων, κάτι ιδιαίτερα απίθανο να συμβεί σε ένα ιδιωτικό BC. Το βασικό πρόβλημα όμως με το δημόσιο BC, είναι οι υψηλές απαιτήσεις σε ενέργεια και αποθηκευτικό χώρο (και άρα κόστος), για τη διατήρηση ενός κατανεμημένου

καθολικού σε μεγάλη κλίμακα, καθώς και ο σχετικά μεγαλύτερος χρόνος ολοκλήρωσης των συναλλαγών, λόγω του χρόνου που χρειάζεται ο μηχανισμός της συναίνεσης[22].

- Ιδιωτικό BC

Από την άλλη πλευρά, η κοινοπραξία ή ο οργανισμός που εκμεταλλεύεται ένα ιδιωτικό BC μπορεί εύκολα, αν το επιθυμεί, να τροποποιήσει τους κανόνες του πρωτοκόλλου, να επαναφέρει συναλλαγές, να διαγράψει δεδομένα κλπ., στοιχείο, που σε ορισμένες περιπτώσεις συνιστά αναγκαιότητα. Επίσης, τα ιδιωτικά BC παρέχουν μεγαλύτερη ευχέρεια επέκτασης/κλιμάκωσης, ενώ και οι κόμβοι που επικυρώνουν τις συναλλαγές είναι γνωστοί, επομένως δεν υφίσταται οποιοσδήποτε κίνδυνος επίθεσης 51% [23], που θα μπορούσε να προέλθει από κάποια αθέμιτη σύμπραξη κόμβων. Επιπλέον, οι συναλλαγές κοστίζουν φθηνότερα -σε όρους ενέργειας και αποθηκευτικού κόστους- και πραγματοποιούνται ταχύτερα, αφού χρειάζεται να επαληθευτούν μόνο από λίγους, ισχυρούς επεξεργαστικά κόμβους και όχι από χιλιάδες, λιγότερο ισχυρούς. Επιπροσθέτως, αν τα δικαιώματα ανάγνωσης των συναλλαγών είναι περιορισμένα, τα ιδιωτικά BC μπορούν να παρέχουν μεγαλύτερο επίπεδο προστασίας της ιδιωτικότητας και συνεπώς, ευχερέστερη συμμόρφωση με τους κανόνες περί προσωπικών δεδομένων (Buterin, 2015). Το βασικό μειονέκτημα όμως αυτής της λύσης είναι ότι όντας λιγότερο αποκεντρωμένη, θέτει τους οργανισμούς σε κίνδυνο παραβίασης της ασφάλειας, ακριβώς όπως σε ένα κλασικό, συγκεντρωτικό σύστημα. Παράλληλα, μειώνεται και η συνολική διαφάνεια του συστήματος, καθώς εγκαθίστανται περιορισμοί στα δικαιώματα πρόσβασης στα δεδομένα.

Τέλος, θα μπορούσε ως επίλογος να προστεθεί και το γεγονός ότι το δημόσιο BC έχει και φιλοσοφικές / αξιακές προεκτάσεις και αποτελεί, μεταξύ άλλων, ένα κίνημα που αμφισβητεί την ίδια την ιδέα του ελέγχου από οργανισμούς και κυβερνήσεις. Υπό αυτή την έννοια μπορεί να θεωρηθεί ακόμα και αναρχικό. Από την άλλη πλευρά, το ιδιωτικό BC είναι το κατεστημένο, απλά προσπαθώντας να καταστήσει τα πράγματα λιγότερο δυσκίνητα και πιο αξιόπιστα (Strukhoff, 2016).

[22]Για παράδειγμα στο bitcoin χρειάζονται 10-12 λεπτά για να επικυρωθεί ένα μπλοκ με συναλλαγές.
[23] βλ. σελ.48 (επίθεση 51%)

2.6. Τρόποι προσέγγισης της τεχνολογίας Blockchain

Οι πιο διαδεδομένοι τρόποι προσέγγισης και εφαρμογής της τεχνολογίας BC από έναν δημόσιο οργανισμό είναι οι εξής: (Blockchain Hub, 2016)

2.6.1. Blockchain as a Service (BaaS)

Οι μεγάλοι παίκτες της βιομηχανίας cloud, όπως η Amazon, η Microsoft (Azure) και η IBM (BlueMix) έχουν αναγνωρίσει τα πιθανά οφέλη από την προσφορά υπηρεσιών BC στο cloud και έχουν ήδη αρχίσει να παρέχουν ένα επίπεδο BaaS σε κάποιους πελάτες τους. Η συγκεκριμένη μέθοδος εφαρμογής του BC είναι επωφελής για τους χρήστες, καθώς δεν θα έχουν να αντιμετωπίσουν το πρόβλημα της διαμόρφωσης και ρύθμισης ενός τέτοιου λειτουργικού περιβάλλοντος. Επίσης, δεν θα χρειαστεί να προβούν σε επενδύσεις σε εξοπλισμό, ενώ επιπλέον, μπορούν να αναπτύξουν εύκολα 'proofs-of-concept' (PoC) [24] και να αρχίσουν να πειραματίζονται, καθιστώντας φθηνότερη και ευκολότερη την υιοθέτηση της τεχνολογίας . Οι υπηρεσίες BaaS που έχουν αναπτυχθεί ή πρόκειται να αναπτυχθούν άμεσα είναι οι εξής:

- Η Microsoft συνεργάζεται με την ConsenSys και προσφέρει την υπηρεσία Ethereum Blockchain ως υπηρεσία (EBaaS) στο Microsoft Azure.
- Η IBM (BueMix) συνεργάζεται με την Hyperledger για να προσφέρει BaaS στους πελάτες της.
- Η Amazon ανακοίνωσε ότι θα προσφέρει την υπηρεσία BaaS σε συνεργασία με την startup Kaleido.

2.6.2. Blockchain πρωτοπόρος

Σε αυτή την περίπτωση, ένας οργανισμός εργάζεται απευθείας με τα ίδια τα εργαλεία του BC. Για παράδειγμα στο Ethereum, με τη γλώσσα Solidity και τα εργαλεία της. Εδώ απαιτείται ανάπτυξη των εφαρμογών από το μηδέν, οπότε αυτή η μέθοδος δεν είναι για όλους, ιδιαίτερα δεδομένου του γεγονότος ότι πολλές από τις τεχνολογίες ακόμα αναπτύσσονται και εξελίσσονται.

[24] Ένα PoC είναι η πρακτική υλοποίηση μιας συγκεκριμένης μεθόδου ή μιας ιδέας, ώστε να αποδειχθεί η χρησιμότητα και η εφικτότητά της.

2.6.3. Κάθετες λύσεις

Σε αυτές τις λύσεις είναι που παρατηρούμε την ταχύτερη εξέλιξη, κυρίως στις χρηματοπιστωτικές υπηρεσίες. Αυτές οι λύσεις είναι προσαρμοσμένες για τον εκάστοτε κλάδο και βασίζονται σε ιδιωτικά και κοινοπρακτικά BC, με τη χρήση APIs (Διεπαφή Προγραμματισμού Εφαρμογών).[25]

[25] Ένας από τους βασικούς σκοπούς μίας διεπαφής είναι να ορίζει και να διατυπώνει το σύνολο των λειτουργιών-υπηρεσιών που μπορεί να παρέχει μια βιβλιοθήκη ή ένα λειτουργικό σύστημα σε άλλα προγράμματα, χωρίς να επιτρέπει πρόσβαση στον κώδικα που υλοποιεί αυτές τις υπηρεσίες. Η διεπαφή διαχωρίζει την προγραμματιστική υλοποίηση κάποιων υπηρεσιών από τη χρήση τους.

3. Το Blockchain στην Ευρωπαϊκή Ένωση

3.1. Η σχέση του BC με τη Στρατηγική της ΕΕ για την Ψηφιακή Ενιαία Αγορά

Η Επιτροπή Γιούνκερ έθεσε προτεραιότητα από τον Μάιο του 2015 την δημιουργία της Ενιαίας Ψηφιακής Αγοράς (European Commission, 2015). Αυτή η στρατηγική, που αποτελεί πρωτοβουλία της στρατηγικής Ευρώπη 2020[26], ήταν απόρροια της συνειδητοποίησης ότι πολύ συχνά οι Ευρωπαίοι πολίτες αντιμετωπίζουν εμπόδια, όταν χρησιμοποιούν διαδικτυακά εργαλεία και υπηρεσίες, ενώ οι διαδικτυακές αγορές εξακολουθούν να περιχαρακώνονται κατά κύριο λόγο στα εθνικά σύνορα όσον αφορά τις διαδικτυακές υπηρεσίες. Στόχος της Επιτροπής Γιούνκερ ήταν η δημιουργία μιας ενιαίας ψηφιακής αγοράς, όπου οι πολίτες και οι επιχειρήσεις θα μπορούν να έχουν απρόσκοπτη πρόσβαση σε διαδικτυακά αγαθά και υπηρεσίες, ανεξαρτήτως εθνικότητας και τόπου διαμονής. Κλειδί για την επίτευξη του ανωτέρου στόχου και την δημιουργία της Ψηφιακής Ενιαίας Αγοράς, που σύμφωνα με υπολογισμούς θα μπορούσε να συνεισφέρει 415 δισ. ευρώ στην ευρωπαϊκή οικονομία, αποτελεί η 'αμοιβαία αναγνώριση' σε όλη την ΕΕ.

Στο πλαίσιο αυτό, είναι προφανές ότι η τεχνολογία BC φαίνεται ιδιαίτερα ελκυστική, καθώς επιτρέπει ασφαλείς και διαδραστικές εφαρμογές, με διαφανείς διαδικασίες, επαληθεύσιμες από όλα τα εμπλεκόμενα μέρη και όπου οι συναλλαγές ολοκληρώνονται με ασφάλεια, αμετάκλητα και χωρίς την ανάγκη των κεντρικών οντοτήτων και των περίπλοκων και δαπανηρών κλειστών συστημάτων τους. Ιδιαίτερα στην περίπτωση της ΕΕ, όλα αυτά είναι ιδιαίτερα σημαντικά, καθώς μια αποκεντρωμένη τεχνολογία όπως αυτή προσιδιάζει στον αποκεντρωμένο χαρακτήρα της ίδιας της δομής της ΕΕ. Εύκολα μπορούμε να φανταστούμε μια τέτοια πλατφόρμα σε πανευρωπαϊκή κλίμακα, με συναλλαγές που θα πραγματοποιούνται διασυνοριακά σε πραγματικό χρόνο και χωρίς μεσάζοντες, με τρόπο που να καθιστά την ενιαία αγορά πραγματικότητα, και μάλιστα, αποφεύγοντας μεγάλο μέρος του σημερινού κατακερματισμού.

[26] Ανακοίνωση της Επιτροπής, της 6ης Μαΐου 2015, με τίτλο «Στρατηγική για την ψηφιακή ενιαία αγορά της Ευρώπης» (COM(2015)0192).

3.2. Δράσεις και Πρωτοβουλίες

Ευρωπαίοι πρωτοπόροι επιχειρηματίες ήδη προσφέρουν κάποιες λύσεις βασισμένες σε BC και σημαντικοί οργανισμοί από παραδοσιακούς τομείς, όπως οι τράπεζες, οι ασφαλιστικές εταιρείες, τα χρηματιστήρια, η εφοδιαστική κ.α. συμμετέχουν σε διάφορα πιλοτικά έργα. Επίσης, πολλά κράτη μέλη έχουν ανακοινώσει πρωτοβουλίες, καθώς επιδιώκουν να ενισχύσουν τη χρήση της συγκεκριμένης τεχνολογίας. Στο πλαίσιο αυτό, η Ευρωπαϊκή Επιτροπή προσπαθεί να ενισχύει τις υπάρχουσες πρωτοβουλίες και να καλλιεργήσει την σχετική τεχνογνωσία.

3.2.1. Horizon 2020

Δεν εκπλήσσει συνεπώς το γεγονός, ότι η Ευρωπαϊκή Επιτροπή χρηματοδοτεί έργα BC, μέσω των ερευνητικών προγραμμάτων FP7[27] και Horizon 2020[28], ήδη από το 2013. Με τα σημερινά δεδομένα, μέχρι το 2020 θα χρηματοδοτήσει έργα που αξιοποιούν τεχνολογίες BC, συνολικού προϋπολογισμού € 340 εκ. ευρώ. (European Commission , 2018)

- Άξονας «Βιομηχανική Υπεροχή» [29]

Συγκεκριμένα, αυτή τη στιγμή, υπό τον άξονα «Βιομηχανική Υπεροχή" του Horizon2020:

α) Είναι ενεργή (μέχρι τον Μάιο του 2019) η πρόσκληση με τίτλο ‘Blockchains for Social Good', με σκοπό την ενίσχυση πρωτοβουλιών που έχουν στόχο την ανάπτυξη αποδοτικών και αποτελεσματικών αποκεντρωμένων λύσεων για την αντιμετώπιση των κοινωνικών προκλήσεων (European Commission, 2018).

β) ‘Εληξε πριν λίγους μήνες (Μάιος 2018) η πρόσκληση με τίτλο ‘Blockchain and distributed ledger technologies (DLT) for SMEs’[30] (European Commission, 2018). Σκοπός της πρόσκλησης ήταν η επιλογή έργων που θα καταφέρουν να βρουν βιώσιμες λύσεις στα

[27] Το FP7 ήταν το πρόγραμμα χρηματοδότησης της έρευνας και της καινοτομίας της Ευρωπαϊκής Ένωσης για την περίοδο 2007-2013 και ήταν πρόδρομος του σημερινού HORIZON 2020.
[28] Το πρόγραμμα "Horizon 2020" είναι το μεγαλύτερο έως σήμερα πρόγραμμα έρευνας και καινοτομίας της ΕΕ με προϋπολογισμό σχεδόν 80 δισ. ευρώ για 7 έτη (2014-2020)
[29] Οι τρεις κύριοι άξονες του προγράμματος είναι: Επιστημονική Αριστεία, Βιομηχανική Υπεροχή, Κοινωνικές Προκλήσεις
[30] Small and Medium Enterprises

μειονεκτήματα της τεχνολογίας DLT, όπως αυτά που σχετίζονται με τη διαλειτουργικότητα, τα πρότυπα και την προστασία των δεδομένων.

- Άξονας «Κοινωνικές Προκλήσεις»

Υπό τον άξονα του Horizon 2020 'Κοινωνικές Προκλήσεις' θα είναι ενεργές, μέχρι τις 15 Μαίου του 2019 οι εξής προσκλήσεις:

α) Πρόσκληση με τίτλο 'Blockchain Enabled Healthcare'. (European Commission, 2018) Σκοπός της πρόσκλησης είναι να αναπτυχθεί ένα ενιαίο οικοσύστημα ανάπτυξης, παρασκευής και διανομής φαρμάκων, βασισμένο στη τεχνολογία BC, που να αντιμετωπίζει τα προβλήματα του κλάδου της φαρμάκου, όπως η πολυπλοκότητα των διαδικασιών και η έλλειψη διαφάνειας.

β) Πρόσκληση με τίτλο 'Socioeconomic and cultural Transformations in the Context of the 4th Industrial Revolution', που εμπεριέχει τον άξονα 'Transformative impact of disruptive technologies in public services', με τον οποίο θα χρηματοδοτηθούν πιλοτικά έργα που θα προσπαθήσουν να αξιολογήσουν το αντίκτυπο των τεχνολογιών που μπορούν να διαταράξουν (disruptive) το υπάρχον μοντέλο παροχής των δημόσιων υπηρεσιών, και να πειραματιστούν με αυτές.

3.2.2. Παρατηρητήριο και Φόρουμ Blockchain

Εκτός από τα χρηματοδοτικά εργαλεία, η ΕΕ εγκαινίασε το Ευρωπαϊκό Παρατηρητήριο και Φόρουμ για το Blockchain τον Φεβρουάριο του 2018. Το Παρατηρητήριο προβλέπεται να βοηθήσει την Ευρώπη να εκμεταλλευτεί τις νέες ευκαιρίες που προσφέρει το BC και να καλλιεργήσει εμπειρογνωμοσύνη στο πεδίο. Ο ρόλος του είναι να συγκεντρώνει πληροφορίες, να παρακολουθεί και να αναλύει τις τάσεις, καθώς και να διερευνήσει το κοινωνικοοικονομικό δυναμικό και αντίκτυπο του BC. (European Commission , 2018) Στο πλαίσιο αυτό, η ConsenSys, μία start-up[31] στην πλατφόρμα του Ethereum, που έχει πλέον εξελιχθεί σε παγκόσμιο οργανισμό ανάπτυξης λύσεων και υποδομών BC, επιλέχθηκε -μετά από πρόσκληση υποβολής προσφορών το 2017- ως εταίρος για να υποστηρίξει τις δράσεις του Παρατηρητηρίου. Όντας σημαντικός παράγοντας στον χώρο του blockchain, η ConsenSys

[31] Νεοφυής επιχείρηση

προβλέπεται να προσδώσει ισχυρή δυναμική στην ανάπτυξη του blockchain στην ΕΕ. (Nicholson, 2018)

3.2.3. Ευρωπαϊκή Εταιρική Σχέση Blockchain (European Blockchain Partnership, EBP)

Επίσης, στις 10 Απριλίου 2018, 21 κράτη μέλη της ΕΕ και η Νορβηγία συμφώνησαν να υπογράψουν μια κοινή δήλωση για τη δημιουργία της Ευρωπαϊκής Εταιρικής Σχέσης Blockchain και να συνεργαστούν για τη δημιουργία μιας ευρωπαϊκής υποδομής υπηρεσιών blockchain (EBSI), η οποία θα υποστηρίζει την παροχή διασυνοριακών ψηφιακών δημόσιων υπηρεσιών , με τα υψηλότερα πρότυπα ασφάλειας και ιδιωτικότητας. Έκτοτε, ακόμα 4 κράτη μέλη[32] έχουν προσχωρήσει στην εταιρική σχέση (European Commission, 2018). Σύμφωνα με την κοινή αυτή δήλωση, η στενή συνεργασία μεταξύ των κρατών μελών θα συμβάλλει στην αποφυγή κατακερματισμένων προσεγγίσεων και θα εξασφαλίσει τη διαλειτουργικότητα και την ευρύτερη ανάπτυξη υπηρεσιών βασισμένων στο blockchain.

3.3. Θεσμικό πλαίσιο στην ΕΕ

Αν και η υλοποίηση της πρώτης εφαρμογής του BC, δηλαδή το bitcoin, εντοπίζεται το 2009 και μέχρι το 2013 είχε λάβει μεγάλες διαστάσεις, εντούτοις, στην Ελλάδα αλλά και στην ΕΕ δεν υπάρχει ακόμα ειδικό νομοθετικό πλαίσιο που να ρυθμίζει τη λειτουργία του συστήματος και την χρήση του Bitcoin, γενικότερα των κρυπτονομισμάτων, αλλά και συνολικά της τεχνολογίας του BC. Η ΕΕ -καθώς και οι κρατικές αρχές των περισσοτέρων κρατών μελών- φαίνεται συγκρατημένη στο να προβεί στη νομοθετική ρύθμιση του φαινομένου (Kastelein, 2018), καθώς δεν επιθυμεί, δρώντας βιαστικά, να πλήξει άθελά της την καινοτομία, να επιβραδύνει την τεχνολογική πρόοδο, και να μείνει πίσω στον τεχνολογικό ανταγωνισμό.

Αναμφίβολα, αυτό που είναι καταρχάς αναγκαίο και αποτελεί προϋπόθεση για τη νομική αντιμετώπιση και την ένταξη της τεχνολογίας BC σε σύνολο κανόνων δικαίου (τουλάχιστον στην εφαρμογή της στα κρυπτονομίσματα), είναι ο νομικός τους χαρακτηρισμός. Διότι, αν και το όνομα παραπέμπει σε νομίσματα, σχεδόν κανένα από τα κρυπτονομίσματα δεν

[32] Η Ελλάδα υπέγραψε στις 23 Μαΐου του 2018.

λειτουργεί ως νόμισμα. Η μόνη σχετική νομοθεσία που θα μπορούσε να αποτελέσει τη βάση για τη ρύθμιση του BC και συγκεκριμένα των εικονικών νομισμάτων είναι, μέχρι στιγμής, η Οδηγία για το ηλεκτρονικό χρήμα 2009/110/ΕΚ[33], όπως ενσωματώθηκε στην ελληνική νομοθεσία με το Ν. 4261/2014[34]. Όμως, το Bitcoin και γενικότερα τα εικονικά νομίσματα διαφέρουν από το ηλεκτρονικό χρήμα, όπως αυτό ορίζεται στην ανωτέρω Οδηγία, καθώς, σε αντίθεση με το ηλεκτρονικό χρήμα, τα χρηματικά ποσά δεν εκφράζονται σε κάποια κρατικά αναγνωρισμένη μονάδα, αλλά σε μια εικονική μονάδα. Στο ίδιο πλαίσιο, σε έκθεσή της το 2012 (European Cental Bank, 2012), η Ευρωπαϊκή Κεντρική Τράπεζα επίσης απορρίπτει την υπαγωγή του Bitcoin στις διατάξεις της άνω Οδηγίας.

Σε επόμενη έκθεσή της, πάντως, (European Central Bank, 2015) η ΕΚΤ όρισε τα εικονικά νομίσματα ως μία ψηφιακή αποτύπωση αξίας, η οποία, σε ορισμένες περιπτώσεις, μπορεί να χρησιμοποιηθεί ως εναλλακτική του – παραδοσιακού – χρήματος. Στο ίδιο πλαίσιο κινείται και το Δικαστήριο της ΕΕ στην υπόθεση C 264/14 (σκέψη 42), σύμφωνα με την οποία, στην περίπτωση ρητής συμφωνίας μεταξύ των συμβαλλομένων μερών, το Bitcoin θα μπορούσε να θεωρηθεί ότι αποτελεί ένα μέσο πληρωμής για τις επιχειρήσεις που το δέχονται. Επίσης, σύμφωνα με την αιτιολογική σκέψη 49, οι πράξεις που αφορούν μη συμβατικά νομίσματα είναι χρηματοπιστωτικές πράξεις, υπό την προϋπόθεση ότι τα εν λόγω μη συμβατικά νομίσματα γίνονται δεκτά από τους συναλλασσόμενους ως εναλλακτικό μέσο πληρωμής.

Από την ανωτέρω ανάλυση συνάγεται ότι αν και μπορούν να γίνουν αποδεκτές οι συναλλαγές σε κρυπτονομίσματα, υπό τη προϋπόθεση ότι οι συναλλασσόμενοι τα αποδέχονται, εντούτοις, τα εικονικά νομίσματα δε μπορούν να θεωρηθούν χρήμα. Τελικά, το ρυθμιστικό πλαίσιο εντός του οποίου μπορεί να λειτουργήσουν τα εικονικά νομίσματα παραμένει ακόμα ασαφές. Σε κάθε περίπτωση, για να είναι δυνατή η πλήρης και αποτελεσματική αξιοποίηση της δυναμικής τους, αλλά και της τεχνολογίας blockchain γενικότερα, η αυτορρύθμιση και η θέσπιση ενός κανονιστικού πλαισίου ρυθμίσεων, που να μην πλήττει την καινοτομία, φαίνεται να είναι η βέλτιστη λύση.

Στο πλαίσιο αυτό κινείται και το ψήφισμα του Ευρωπαϊκού Κοινοβουλίου τον Οκτώβριο του 2018, όπου συνοπτικά, επισημαίνεται ότι οποιαδήποτε κανονιστική ρύθμιση της τεχνολογίας DLT θα πρέπει να είναι φιλική προς την καινοτομία, θα πρέπει να επιτρέπει τη μεταβίβαση σε αυτή και θα πρέπει να καθοδηγείται από τις αρχές της ουδετερότητας της

[33] Οδηγία 2009/110/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Σεπτεμβρίου 2009, για την ανάληψη, άσκηση και προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος.

[34] (ΦΕΚ Α' 107/5-5-2014). Πρόσβαση στη δραστηριότητα των πιστωτικών ιδρυμάτων και προληπτική εποπτεία πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων, κατάργηση του ν. 3601/2007 και άλλες διατάξεις.

τεχνολογίας και της ουδετερότητας των επιχειρηματικών μοντέλων. (European Parliament, 2018)

3.4. Πρόσθετες νομικές πτυχές

Κάποιες επιπρόσθετες, σημαντικές νομικές πτυχές της τεχνολογίας BC είναι, μεταξύ άλλων, οι παρακάτω:

3.4.1. Προσωπικά δεδομένα

Όπως είναι φυσιολογικό, η νέα τεχνολογία, ως ένας νέος τρόπος καταχώρησης και αποθήκευσης δεδομένων, θα πρέπει καταρχάς να εξεταστεί υπό το πρίσμα του δικαίου της προστασίας προσωπικών δεδομένων και της πιο πρόσφατης ευρωπαϊκής νομοθεσίας, δηλαδή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ)[35]. Προκειμένου να πετύχει τους σκοπούς του, ο ΓΚΠΔ ενισχύει και εισάγει μια σειρά ψηφιακών δικαιωμάτων, όπως για παράδειγμα είναι, μεταξύ άλλων, το δικαίωμα διαγραφής ("right to erasure") των προσωπικών δεδομένων, το οποίο συνίσταται στη δυνατότητα του ατόμου να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή προσωπικών δεδομένων που το αφορούν[36].

Όμως, στο πλαίσιο μιας ανοιχτής αποκεντρωμένης πλατφόρμας BC παραμένουν ερωτήματα, όπως για παράδειγμα, ποιος θεωρείται ο υπεύθυνος της επεξεργασίας και ποιος ο εκτελών την επεξεργασία, όπου είναι δύσκολο να απαντηθούν. Αλλά και δικαιώματα πρόσβασης, ενημέρωσης και πολύ περισσότερο φορητότητας των υποκειμένων προσωπικών δεδομένων είναι αμφίβολο αν και με ποιό τρόπο θα μπορούσαν να ικανοποιηθούν σε μία βάση δεδομένων, η οποία τηρείται ταυτόχρονα σε χιλιάδες αντίτυπα και από την οποία είναι αδύνατον να τροποποιηθούν, πόσο μάλλον να αφαιρεθούν δεδομένα. Στο πλαίσιο του BC δεν υπάρχει εξ' ορισμού η δυνατότητα διαγραφής, όπως υπάρχει στις κλασικές βάσεις δεδομένων[37], άρα, σε περίπτωση αποθήκευσης προσωπικών δεδομένων στο BC, φαίνεται εξαρχής μια αδυναμία συμμόρφωσης με τον ΓΚΠΔ.

[35] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
[36] Άρθρο 17 του ΓΚΠΔ
[37] Σε αυτές υπάρχουν οι λειτουργίες CRUD (Create-Read-Update-Delete)

Μια δημοφιλής πρόταση για να αντιμετωπιστεί αυτό το πρόβλημα είναι να αποθηκεύονται τα προσωπικά δεδομένα εκτός του BC, στις εξωτερικές βάσεις δεδομένων των οργανισμών και να αποθηκεύεται ο δείκτης προς αυτά τα δεδομένα, μαζί με τη σύνοψή τους (hash) και άλλα μεταδεδομένα στο BC. Σε περίπτωση ανάγκης τροποποιήσεων ή και αιτήματος διαγραφής των δεδομένων αυτών από τον κάτοχό τους, αυτά θα διαγράφονταν κανονικά από την εξωτερική βάση δεδομένων και έτσι, το hash τους στο BC δεν θα αντιπροσωπεύει πλέον τίποτα, δηλαδή θα είναι απλά ένας άνευ νοήματος αριθμός.

Αυτή η λύση, αν και πράγματι παρέχει τη δυνατότητα συμμόρφωσης με τον ΓΚΠΔ, εντούτοις ενέχει σημαντικά μειονεκτήματα, που μειώνουν την χρησιμότητα της τεχνολογίας BC. Για παράδειγμα, με αυτή τη λύση τορπιλίζεται η διαφάνεια, καθώς με την αποθήκευση των δεδομένων εκτός αλυσίδας, δεν υπάρχει κανένας τρόπος να γνωρίζει κάποιος με βεβαιότητα ποιός έχει πρόσβαση στα δεδομένα του. Επίσης, καθώς κάθε εταιρεία έχει τη δική της υποδομή, με τον διασκορπισμό των προσωπικών δεδομένων σε αυτές τις διαφορετικές υποδομές, αυξάνεται ο κίνδυνος και η πιθανότητα για ενδεχόμενη παραβίαση και κλοπή των δεδομένων, ακριβώς όπως στα κεντρικά συστήματα αποθήκευσης.

3.4.2. Δίκαιο προστασίας καταναλωτή

Η πλέον δημοφιλής, σήμερα, εφαρμογή της τεχνολογίας blockchain, τα κρυπτονομίσματα, εγείρουν σημαντικά ζητήματα που άπτονται του δικαίου του καταναλωτή, λόγω ορισμένων μειονεκτημάτων που παρουσιάζουν και ειδικότερα:

- Έλλειψη διαφάνειας ως προς τον τρόπο λειτουργίας τους, καθώς τα βασικά χαρακτηριστικά τους είναι δυσνόητα για τους χρήστες ενώ οι διαθέσιμες πληροφορίες είναι περιορισμένες. Επιπλέον, καθώς οι περισσότεροι χρήστες επενδύουν σε αυτά, προσβλέποντας στην αύξηση της αξίας τους, είναι πιθανό να πέσουν θύματα απατηλών υποσχέσεων από τους εκδότες.
- Το νομικό καθεστώς των κρυπτονομισμάτων είναι ασαφές, όπως είναι συχνά και η ταυτότητα των βασικών παραγόντων αυτών, οι οποίοι κατά κανόνα δεν υπάγονται σε ρύθμιση ή επίβλεψη. Επομένως, οι χρήστες δεν επωφελούνται νομικών προβλέψεων προστασίας, όπως ενός συστήματος εγγύησης των καταθέσεων και είναι εκτεθειμένοι σε διάφορους κινδύνους.
- Τέλος, η συνέχεια ενός εικονικού νομίσματος κάθε άλλο παρά εγγυημένη είναι και οι χρήστες είναι πιθανόν να βρεθούν αντιμέτωποι με απότομη διακοπή της έκδοσης ή ισχύος του εικονικού νομίσματος. (Λογαράς, 2018)

4. Επιχειρησιακή Ανάλυση

4.1. Ανάλυση SWOT

Από την προηγούμενη ανάλυση είναι δυνατόν να εντοπιστούν κάποια σημαντικά πλεονεκτήματα και ευκαιρίες που παρουσιάζει η τεχνολογία του BC, που αποτελούν ουσιαστικά και την προστιθέμενη αξία της τεχνολογίας για τη κοινωνία. Επίσης, είναι εφικτό να εντοπιστούν κάποια κρίσιμα μειονεκτήματα, αλλά και οι απειλές που εμφιλοχωρούν στη συγκεκριμένη τεχνολογία. Είναι σημαντικό να επισημανθεί ότι η ανάλυση που ακολουθεί αφορά κυρίως το δημόσιο BC, καθώς το ιδιωτικό και κοινοπρακτικό BC καταφέρνουν να αποφύγουν τα περισσότερα αρνητικά, με σημαντικές υποχωρήσεις όμως, όπως έχουν επισημανθεί προηγουμένως.

4.1.1. Πλεονεκτήματα

- Ενισχυμένη ασφάλεια και αμεταβλητότητα

Σε ένα BC οι συναλλαγές πρέπει να συμφωνηθούν (μηχανισμός συναίνεσης) πριν καταγραφούν. Μετά την έγκριση μιας συναλλαγής, αυτή κρυπτογραφείται και συνδέεται με την προηγούμενη συναλλαγή. Το γεγονός αυτό, μαζί με την αποθήκευση των πληροφοριών σε ένα δίκτυο πολλών κόμβων (υπολογιστών), καθιστά ιδιαίτερα δύσκολη την υπονόμευση των δεδομένων της συναλλαγής (Hooper, 2018). Επίσης, η αμεταβλητότητα των δεδομένων, λόγω της πολλαπλής αποθήκευσης τους σε πολλά αντίγραφα είναι συνδεδεμένη με την ασφάλεια και τις βασικές αρχές της, την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα, καθώς δημιουργεί τις προϋποθέσεις για ενισχυμένη εμπιστοσύνη στην ακεραιότητα των δεδομένων και ελαχιστοποιεί τις πιθανότητες για απάτη.

- Μικρότερη πιθανότητα αποτυχίας του συστήματος

Επίσης, η αποκεντρωμένη δομή του BC οδηγεί σε μικρότερη πιθανότητα αποτυχίας, επειδή βασίζεται σε πολλά ξεχωριστά και διασκορπισμένα στοιχεία και όχι σε ένα κεντρικό. Εάν ένας κόμβος - ή ακόμα και 100 κόμβοι- παύσει να λειτουργεί, το BC επιβιώνει,

υποθέτοντας ότι υπάρχει τουλάχιστον ένας πλήρης κόμβος σε λειτουργία, γεγονός, που το καθιστά ιδιαίτερα ανθεκτικό (Consensys, 2018).

- Αυξημένη διαφάνεια

Επειδή το BC είναι ένας τύπος κατανεμημένου βιβλιαρίου συναλλαγών, όλοι οι συμμετέχοντες στο δίκτυο μοιράζονται τις ίδιες πληροφορίες. Αυτή η 'κοινή έκδοση' του βιβλιαρίου μπορεί να ενημερωθεί μόνο συλλογικά, μέσω συναίνεσης, πράγμα που σημαίνει ότι όλοι πρέπει να συμφωνήσουν σε αυτήν. Έτσι, τα δεδομένα στο BC χαρακτηρίζονται από μεγαλύτερη συνέπεια, ακρίβεια και διαφάνεια, σε σχέση με άλλα συστήματα, ενώ είναι επίσης διαθέσιμα σε όλους τους συμμετέχοντες που έχουν δυνατότητα πρόσβασης.

- Μικρή πιθανότητα εκμετάλλευσης από κακόβουλους χρήστες

Λόγω της αρχιτεκτονικής του συστήματος και του τρόπου που λειτουργεί ο μηχανισμός της συναίνεσης, είναι εξαιρετικά δύσκολο -σε ένα δημόσιο BC- να επωφεληθούν οι χρήστες με κακόβουλη πρόθεση από τους υπόλοιπους. Κάτι τέτοιο θα απαιτούσε, οι κακόβουλοι χρήστες να αποκτήσουν τον έλεγχο του 51% του συνολικού δικτύου, κάτι εξαιρετικά δύσκολο.[38]

- Αυξημένη αποτελεσματικότητα, ταχύτητα και μειωμένο κόστος

Οι παραδοσιακές διαδικασίες είναι συχνά χρονοβόρες και επιρρεπείς στο ανθρώπινο λάθος, ενώ συχνά απαιτούν τη διαμεσολάβηση τρίτου. Με τον εξορθολογισμό και την αυτοματοποίηση αυτών των διαδικασιών με το BC, οι συναλλαγές ολοκληρώνονται ταχύτερα και αποτελεσματικότερα. Και καθώς η αποθήκευση των αρχείων πραγματοποιείται σε ένα ενιαίο βιβλιάριο συναλλαγών, κοινό σε όλους τους συμμετέχοντες, υφίσταται καλύτερη οργάνωση και καλλιεργείται ευκολότερα εμπιστοσύνη, χωρίς να χρειάζονται πολλοί ενδιάμεσοι για την ολοκλήρωση μιας συναλλαγής. Η αυξημένη ταχύτητα και η εξάλειψη των τρίτων σημαίνει σημαντική εξοικονόμηση σε χρήμα. (Deloitte, 2017)

[38] Βλ. σελ. 48: 'Επίθεση 51%'

4.1.2. Ευκαιρίες

- Δίνει τον έλεγχο στον ίδιο τον χρήστη

Επί του παρόντος, ένας χρήστης του Διαδικτύου δεν μπορεί να είναι σίγουρος για το πού και πώς χρησιμοποιούνται τα προσωπικά του δεδομένα. Όμως, με το BC, οι χρήστες μπορούν να ελέγχουν τον τρόπο χρήσης και πρόσβασης στα δεδομένα τους, αφού μόνο αυτοί κατέχουν τα κρυπτογραφικά κλειδιά που απαιτούνται για αυτά. Αυτό σημαίνει μεγαλύτερη κυριαρχία του ατόμου στα δεδομένα που του ανήκουν (self-sovereignty).

- Παρέχει μια πλατφόρμα για Μεγάλα Δεδομένα και την αναλυτική έρευνα

Ήδη βρισκόμαστε σε μια εποχή όπου κάθε ημέρα δημιουργείται ένας απίστευτος όγκος δεδομένων, κλίμακας Petabyte[39], από διάφορες συσκευές (Η/Υ, κινητά τηλέφωνα, αισθητήρες κ.α.) και σε διάφορες μορφές (logs, εικόνες, έγγραφα κ.α.). Στο πλαίσιο αυτό, η τεχνολογία δημόσιου BC, με την δυνατότητα να φέρνει σε κοινό έδαφος μια ποικιλία οργανισμών, από διαφορετικές βιομηχανίες και κλάδους, μπορεί να διαδραματίσει τον ρόλο μιας πλατφόρμας, στην οποία θα βρίσκονται διαθέσιμα -ή θα δημιουργείται η ζήτηση- για μεγάλα δεδομένα, τα οποία, εκτός από ομαδοποιημένα, θα είναι και ανωνυμοποιημένα, λόγω των εγγενών δυνατοτήτων ψευδωνυμοποίησης του BC. Σε ένα τέτοιο πλαίσιο, με μεγάλης κλίμακας ανωνυμοποιημένα δεδομένα, διαθέσιμα σε όποιον τα ζητήσει και προσφέρει την υπολογιστική του ισχύ για αυτά, θα δημιουργηθούν εντελώς νέες δυνατότητες στην αναλυτική έρευνα.

- Τα έξυπνα συμβόλαια μπορούν να οδηγήσουν στη δημιουργία νέων επιχειρηματικών μοντέλων

Είναι γεγονός ότι τα έξυπνα συμβόλαια, έχοντας τις συμβατικές προϋποθέσεις και τους όρους αποτυπωμένους σε κώδικα και αυτόματα υλοποιήσιμους τη στιγμή που ικανοποιείται κάποια ρητά διατυπωμένη συνθήκη, καθιστούν απαρχαιωμένες μια σειρά από οντότητες που είναι σήμερα απαραίτητες για την διασφάλιση της εμπιστοσύνης. Αυτή η εξέλιξη είναι βέβαιο ότι θα γεννήσει νέες επιχειρηματικές ιδέες και επιχειρηματικά μοντέλα σε ένα ευρύ πεδίο δραστηριοτήτων, από τις πληρωμές και την εφοδιαστική αλυσίδα, μέχρι το εμπόριο, τα πνευματικά δικαιώματα και την ακίνητη περιουσία.

[39] 1 Petabyte = 1.000.000 Gigabyte

4.1.3. Αδυναμίες

Όπως όλες οι τεχνολογίες, έτσι και η τεχνολογία BC χαρακτηρίζεται τόσο από πλεονεκτήματα, όσο και από αδυναμίες. Σε μία θεματική έκθεση της εταιρείας μελετών Global Data (Global Data, 2018) για την τεχνολογία BC, που διήρκεσε 18 μήνες και περιελάμβανε συνεντεύξεις με στελέχη από περίπου 100 διαφορετικούς οργανισμούς, υποστηρίζεται η άποψη ότι το BC, αν και έχει κάποια αξία, εντούτοις έχει λάβει διαστάσεις 'φούσκας' και θα 'σκάσει', το αργότερο μέχρι το 2025. Η GlobalData προσθέτει ότι η τεχνολογία DLT είναι πολύπλοκη στην υλοποίηση, εξαιρετικά δαπανηρή στη λειτουργία της και δεν μπορεί συνεπώς να αντικαταστήσει τις σύγχρονες τεχνολογίες ΒΔ σε ευρεία κλίμακα. Πιο αναλυτικά:

- Εξαιρετικά ενεργοβόρα και απαιτητική σε κόστος αποθήκευσης

Η τεχνολογία BC ενέχει υψηλά κόστη αποθήκευσης, καθώς το συνολικό BC πρέπει να αποθηκεύεται σε κάθε κόμβο του δικτύου. Για αυτόν τον λόγο, όλο και περισσότερο χρησιμοποιείται μία προσέγγιση όπου μια συναλλαγή περιλαμβάνει τόσο δεδομένα εντός του BC, όσο και εκτός (off-chain).[40] Ακόμα και με αυτόν τον τρόπο όμως, το πρόβλημα δεν αντιμετωπίζεται πλήρως.

Παράλληλα, τα δημόσια BC έχουν εξαιρετικά υψηλές απαιτήσεις υπολογιστικής ισχύος και ενέργειας. Πράγματι, σύμφωνα με την έκθεση έχει υπολογιστεί ότι μια ολοκληρωμένη συναλλαγή bitcoin απαιτεί περίπου 5.000 φορές περισσότερη ενέργεια από μια ολοκληρωμένη συναλλαγή Visa, λόγω της απαίτησης επίτευξης της συναίνεσης από όλο το δίκτυο (με τον συνηθισμένο μηχανισμό Proof Of Work). Σε έναν κόσμο όμως, όπου η κλιματική αλλαγή έχει ήδη αρχίσει να εκδηλώνεται με καταστροφικά αποτελέσματα και όπου γίνονται προσπάθειες η ανθρωπότητα να μεταβάλει το παραγωγικό της μοντέλο, η τεχνολογία BC, εφαρμοσμένη σε μεγάλη κλίμακα, φαντάζει ως μια στρεβλή οπισθοδρόμηση.

- Ελλιπή συμμόρφωση με τον ΓΚΠΔ

Σε αντίθεση με τα δεδομένα της συναλλαγής, τα ίδια τα αρχεία πρέπει τελικά να αποθηκεύονται τις περισσότερες φορές σε εξωτερικές βάσεις δεδομένων. Μία από τις αιτίες

[40] Δηλαδή, αντί να ψηφιοποιείται όλο το στοιχείο και να αποθηκεύεται στο BC, αποθηκεύεται μόνο το hash του και το στοιχείο παραμένει σε μια εξωτερική ΒΔ. .Και για μεγαλύτερη εξοικονόμηση χώρου, χρησιμοποιείται η κρυπτογραφική τεχνική του Δέντρου Merkle, όπου ουσιαστικά ομαδοποιούνται τα hash όλων των συναλλαγών ενός μπλοκ σε ένα μόνο hash.

γι’ αυτό -εκτός από τις απαιτήσεις σε αποθηκευτικό χώρο- είναι ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων της ΕΕ, ο οποίος, μεταξύ άλλων, ορίζει ότι οι υπεύθυνοι επεξεργασίας που διαχειρίζονται προσωπικά δεδομένα πολιτών της ΕΕ, πρέπει να επιτρέπουν τη διαγραφή των προσωπικών δεδομένων, εφόσον τους ζητηθεί. Αυτό όμως φαντάζει εξαιρετικά δύσκολο σε μία αποκεντρωμένη βάση δεδομένων, όπως το BC.

- Ελλιπής προστασία χρηστών

Επιπροσθέτως, όπως έχει ήδη αναλυθεί, σε ένα BC δεν υπάρχει προστασία του χρήστη της υπηρεσίας. Σε αντίθεση, σε μια τράπεζα για παράδειγμα, υπάρχει συγκεκριμένη διαδικασία για να μπορέσει ο χρήστης της υπηρεσίας να αμφισβητήσει μια συναλλαγή. (Levine, 2018)

- Ελλιπής διακυβέρνηση και απουσία τεχνικών προτύπων

Σε σχέση και με το ανωτέρω σημείο, μια άλλη αδυναμία είναι η ελλιπής ανάπτυξη σχετικών τεχνικών προτύπων και κοινού πλαισίου διακυβέρνησης του BC. Από ότι φαίνεται, το πιθανότερο είναι ότι σε κάθε κλάδο της αγοράς -στην αρχή τουλάχιστον- δεν θα είναι μόνο ένα αποδεκτό και λειτουργικό σύστημα BC, αλλά αντιθέτως, θα υφίστανται και θα λειτουργούν πολλά και διαφορετικά ιδιωτικά BC, λόγω της ανταγωνιστικής φύσεως της αγοράς. Συνεπώς, οι οργανισμοί θα κληθούν εκ των πραγμάτων να συμφωνήσουν και να καθορίσουν σχετικά πρότυπα και πλαίσιο διακυβέρνησης, υπό τη πίεση ιδίως της ανάγκης ύπαρξης διαλειτουργικότητας μεταξύ τους. (DHL Trend Research, 2018)

4.1.4. Απειλές

- Δυσκολία επεκτασιμότητας

Με κάθε συναλλαγή, το BC προσθέτει ένα ακόμα μπλοκ στην αλυσίδα των συναλλαγών και κάθε μπλοκ περιέχει όλο και περισσότερα δεδομένα, καθώς μεταφέρει όλο το ιστορικό των συναλλαγών πριν από αυτό. Έτσι, καθώς αυξάνεται ο αριθμός των χρηστών και το ιστορικό των συναλλαγών μεγαλώνει, το σημερινό σύστημα κινδυνεύει να λυγίσει από το ίδιο του το βάρος. Διότι καθώς τα μπλοκ αυξάνονται, χρειάζεται περισσότερος χρόνος για να

ολοκληρωθεί κάθε συναλλαγή, εφόσον απαιτείται επαλήθευση από τους χρήστες.[41] Επίσης, για να αντιμετωπιστεί η αυξημένη κίνηση που προκαλείται από τους όλο και περισσότερους χρήστες και συναλλαγές, απαιτούνται περισσότεροι πλήρεις κόμβοι, με το κόστος λειτουργίας που αυτοί συνεπάγονται.

- Επίθεση 51% και ανεπιθύμητη συγκέντρωση

Όπως έχει αναλυθεί προηγουμένως, είναι εξαιρετικά δύσκολο το ενδεχόμενο εκμετάλλευσης από κακόβουλους χρήστες, λόγω της αρχιτεκτονικής του συστήματος και του τρόπου που λειτουργεί ο μηχανισμός συναίνεσης. Αυτό όμως δε σημαίνει πως ένα τέτοιο ενδεχόμενο δεν μπορεί να συμβεί[42]. Στο bitcoin, για παράδειγμα, αυτό θεωρητικά απαιτεί μια ομάδα miners να κατορθώσει να ελέγξει πάνω από το 50% της 'εξόρυξης' bitcoin, δηλαδή της υπολογιστικής ισχύος, όλου του δικτύου. Σε αυτή την περίπτωση οι συγκεκριμένοι miners θα είναι σε θέση να εμποδίσουν -αν επιθυμούν- νέες συναλλαγές και θα ήταν επίσης σε θέση να αντιστρέψουν τις συναλλαγές που ολοκληρώθηκαν, ενώ είχαν υπό τον έλεγχό τους το δίκτυο. Δηλαδή, θα μπορούσαν να επικυρώσουν μια συναλλαγή και στη συνέχεια να την αντιστρέψουν, εμφανιζόμενοι να έχουν ακόμα τα bitcoin της συναλλαγής. Αυτή η ευπάθεια, γνωστή ως 'διπλή δαπάνη', είναι το ψηφιακό ισοδύναμο μιας τέλειας πλαστογραφίας και το πρωταρχικό πρόβλημα που το BC είχε στόχο να αντιμετωπίσει (Investopedia, 2018). Είναι γεγονός ότι αυτός ο κίνδυνος, που σχετίζεται άμεσα με την ανεπιθύμητη συγκέντρωση των miners, είναι περισσότερο υπαρκτός σήμερα, από ότι στο παρελθόν. Στις μέρες μας έχει παρατηρηθεί μία υπερσυγκέντρωση των miners σε ελάχιστα mining pools, όπου η πλειοψηφία -περίπου το 60%- βρίσκεται στην Κίνα, παρέχοντας δυνητικά σε Κινεζικά συμφέροντα τη δυνατότητα ελέγχου των συναλλαγών που επικυρώνονται στα δημόσια BC (Tuwiner, 2018).

- Κβαντικοί υπολογιστές

Υπάρχει πιθανότητα στο μέλλον, αν υλοποιηθούν οι κβαντικοί υπολογιστές, να αποκτήσουν τέτοια ισχύ, ώστε να είναι σε θέση να αποκρυπτογραφήσουν τα δεδομένα που βρίσκονται αποθηκευμένα σε ένα BC.

[41] Επί του παρόντος, το Bitcoin blockchain δημιουργεί ένα μπλοκ, δηλαδή περίπου 2.000-3.000 συναλλαγές, κάθε 10-12 λεπτά. Για λόγους σύγκρισης, το σύστημα της VISA εκκαθαρίζει 47.000 συναλλαγές το δευτερόλεπτο.

[42] Για παράδειγμα,τα blockchain Krypton και Shift, που είναι βασισμένα στα ethereum, υπέστησαν επιθέσεις 51% τον Αύγουστο του 2016, ενώ τον Μάιο του 2018, το κρυπτονόμισμα Bitcoin Gold,υπέστη επίσης τέτοια επίθεση, με τους κακόβουλους χρήστες να καρπώνονται 18 εκατ. δολάρια.

- Πιθανότητα μη ευρείας αποδοχής

Η μικρή αποδοχή της νέας τεχνολογίας φαίνεται να είναι ένα από τα μεγαλύτερα εμπόδια. Για την υπερσκέλιση αυτού του εμποδίου απαιτείται συνεχής ενημέρωση και εκπαίδευση. Ενδεικτικό είναι ότι σύμφωνα με την έρευνα της Gartner (Gartner, 2018), μόνο το 1% των Chief Information officer (CIO) ανέφεραν κάποια μορφή υιοθέτησης της τεχνολογίας BC στο πλαίσιο των οργανισμών τους, ενώ μόνο το 8% των CIO ήταν σε επίπεδο προγραμματισμού ή ενεργού πειραματισμού με την τεχνολογία αυτή.

Συνοψίζοντας την ανωτέρω ανάλυση, είναι εφικτό να σχεδιαστεί ένας πίνακας ανάλυσης SWOT με τις βασικότερες διαστάσεις, όπως αναφέρθηκαν:

Πλεονεκτήματα	Αδυναμίες	Ευκαιρίες	Απειλές
Ενισχυμένη ασφάλεια	Εξαιρετικά ενεργοβόρα	Έλεγχος στον ίδιο τον χρήστη	Δυσκολία επεκτασιμότητας
Μικρότερη πιθανότητα αποτυχίας του συστήματος	Ελλιπή συμμόρφωση με τον ΓΚΠΔ	Πλατφόρμα για Μεγάλα Δεδομένα	Επίθεση 51% και ανεπιθύμητη συγκέντρωση
Αυξημένη διαφάνεια και ιχνηλασιμότητα	Ελλιπής προστασία χρηστών	Νέα επιχειρηματικά μοντέλα	Κβαντικοί υπολογιστές
Μικρή πιθανότητα εκμετάλλευσης από κακόβουλους χρήστες	Ελλιπής διακυβέρνηση και απουσία τεχνικών προτύπων		Πιθανότητα μη ευρείας αποδοχής
Αυξημένη αποτελεσματικότητα, ταχύτητα και μειωμένο κόστος			

Εικόνα 06: Ανάλυση SWOT του Blockchain

4.2. Η τεχνολογία blockchain στον Κύκλο Υπερβολής (hype cycle) της Gartner

Σε έκθεση της συμβουλευτικής εταιρείας Gartner για το Blockchain (Furlonger & Kandaswamy, 2018), επισημαίνεται ότι, αν και εξελίσσονται οι τεχνικές δυνατότητες του blockchain, εντούτοις, η πραγματικότητα δεν συνάδει με τις διαστάσεις της δημοσιότητας που έχει προσλάβει, ενώ οι δυνατότητες που παρέχει δεν προσφέρονται ακόμα για υλοποιήσεις σε

κρίσιμες επιχειρηματικές διαδικασίες. Πιο συγκεκριμένα, αναλύεται η συγκεκριμένη τεχνολογία βάσει του Κύκλου Υπερβολής (Hype Cycle). Ο Κύκλος Υπερβολής της Gartner είναι μια γραφική απεικόνιση των τάσεων στην τεχνολογία και τη καινοτομία, που χρησιμοποιείται ως εργαλείο, κυρίως για την παρακολούθηση της ωριμότητας μιας τεχνολογίας και των μελλοντικών της δυνατοτήτων. Οι φάσεις του Κύκλου Υπερβολής είναι οι εξής:

- **Technology Trigger** : μια ανακάλυψη, η έναρξη διάθεσης ενός προϊόντος ή κάποιο άλλο γεγονός που προκαλεί τη προσοχή (στη περίπτωσή μας η έναρξη του bitcoin και κατόπιν του ethereum).

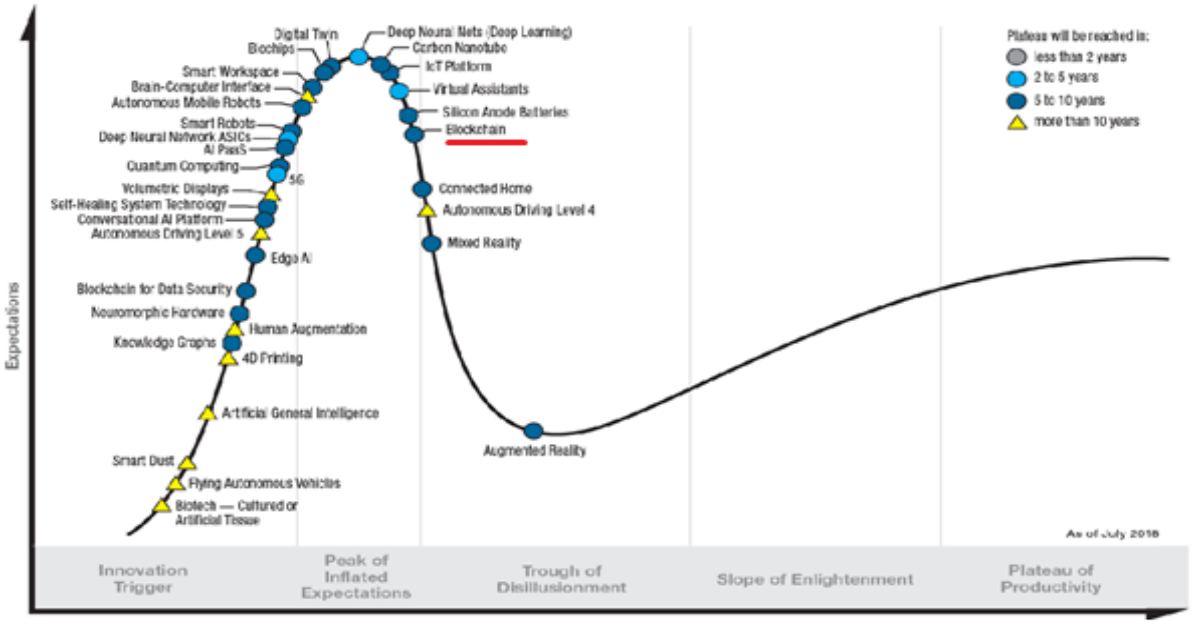
- **Peak of Inflated Expectations** : μια φάση υπερβολικού ενθουσιασμού και μη ρεαλιστικών προσδοκιών, λόγω των δημοσιοποιημένων πρώιμων επιτυχιών της τεχνολογίας, από την οποία όμως δεν λείπουν και οι αποτυχίες (στη περίπτωσή μας η μικρή ανάπτυξη των PoC έργων) καθώς η τεχνολογία δεν είναι ώριμη.

- **Trough of Disillusionment** : η τεχνολογία δεν ανταποκρίνεται στις υπερβολικές προσδοκίες και γρήγορα χάνει την αρχική αίγλη της. Πράγματι, στη περίπτωση που μας ενδιαφέρει, είναι χαρακτηριστικό ότι σύμφωνα με την Gartner, μόλις το 15% των σχετικών επιχειρηματικών προσπαθειών επιβιώνει μετά τον πρώτο χρόνο, ενώ και στο Github[43], τα έργα που σχετίζονται με το BC, αν και αγγίζουν τις 8.600/έτος, έχουν μέση διάρκεια ζωής 1,2 έτη και μόλις το 8% είναι ενεργά (Trujillo, et al., 2017). Σύμφωνα με την Gartner, σε αυτή τη φάση βρίσκεται τώρα η τεχνολογία BC.

- **Slope of Enlightenment** : οι πειραματισμοί και οι επίπονες προσπάθειες από διάφορους οργανισμούς ποικίλου φάσματος οδηγούν στη κατανόηση των πραγματικών δυνατοτήτων της τεχνολογίας, των κινδύνων και των ωφελειών της.

- **Plateau of Productivity** : τα πραγματικά οφέλη της τεχνολογίας γίνονται ευρέως αποδεκτά, ενώ τα σχετικά εργαλεία και οι μεθοδολογίες σταθεροποιούνται.

[43] Η μεγαλύτερη διαδικτυακή πλατφόρμα ανάπτυξης λογισμικού



Εικόνα 06: Κύκλος Υπερβολής Gartner του Blockchain (για το 2018)

4.3. Κρίσιμοι Παράγοντες Επιτυχίας

Είναι σημαντικό να γίνει κατανοητό ότι η τεχνολογία BC δεν αποτελεί την ιδανική επιλογή σε κάθε περίπτωση. Λαμβάνοντας υπόψη και την έως τώρα ανάλυση είναι εφικτό να προσδιορίσουμε τους κρίσιμους παράγοντες επιτυχίας για την επιλογή ή μη της συγκεκριμένης τεχνολογίας:

4.3.1. Καταλληλότητα της τεχνολογίας

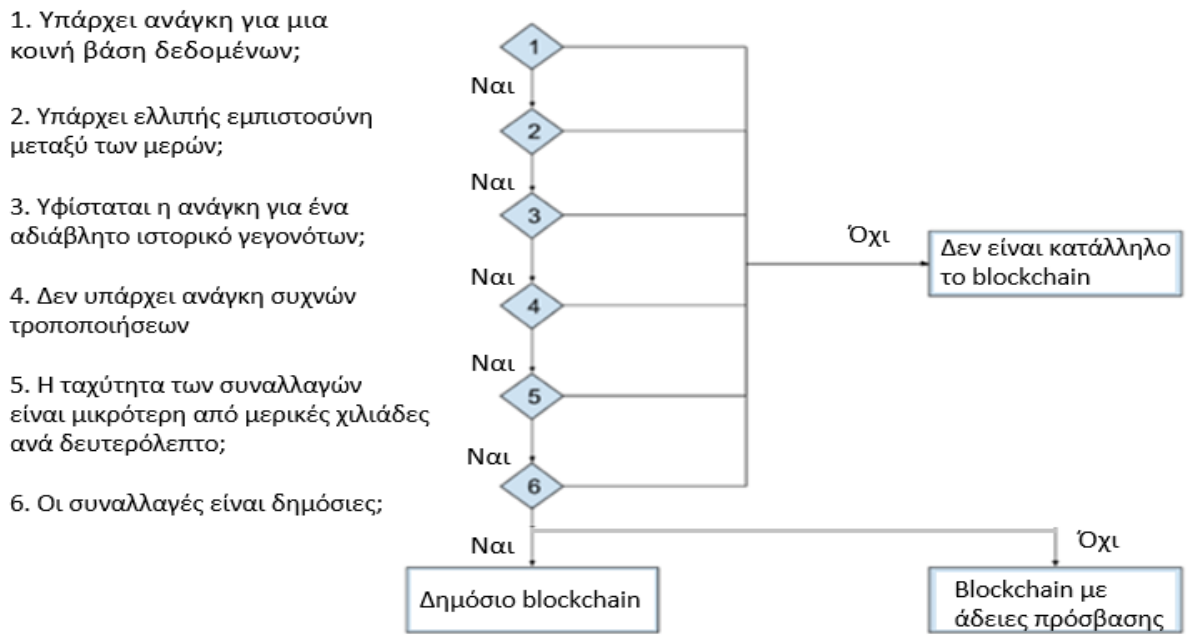
Αναμφίβολα, ένας από τους κρισιμότερους παράγοντες είναι να υφίστανται οι συνθήκες εκείνες, στις οποίες η τεχνολογία BC προσφέρει συγκριτικό πλεονέκτημα. Δεδομένης της ανάλυσης που έχει προηγηθεί, διαπιστώνουμε ότι η τεχνολογία BC είναι καλύτερα προσαρμοσμένη για τις περιπτώσεις όπου ισχύουν κάποιες ή όλες οι παρακάτω συνθήκες: (Paul, 2017)

- Υπάρχει ανάγκη για μια κοινή βάση δεδομένων.
- Τα μέρη που συμμετέχουν στο σύστημα έχουν αντικρουόμενα κίνητρα ή δεν υφίσταται επαρκής εμπιστοσύνη μεταξύ τους.

- ➢ Υπάρχουν ενιαίοι κανόνες που διέπουν τους συμμετέχοντες στο σύστημα.
- ➢ Δεν υπάρχει ανάγκη για συχνές τροποποιήσεις και αλλαγές στα δεδομένα.
- ➢ Υφίσταται ανάγκη για ένα ακέραιο και αδιάβλητο ιστορικό γεγονότων.
- ➢ Η ταχύτητα των συναλλαγών δεν υπερβαίνει τις μερικές χιλιάδες ανά λεπτό.

Αν πρόκειται για έναν μόνο οργανισμό ή για μια μικρή ομάδα οργανισμών μεταξύ των οποίων επικρατούν σχέσεις εμπιστοσύνης και κοινοί κανόνες, είναι πιθανό η λύση μιας σχεσιακής βάσης δεδομένων να αποτελεί καταλληλότερη επιλογή. Επιπλέον, εάν υφίσταται ανάγκη συχνής αλλαγής ή\και διαγραφής των δεδομένων, τότε πρέπει να εξεταστεί προσεκτικά εάν το BC αποτελεί τη βέλτιστη επιλογή, καθώς οι "τροποποιήσεις" στα δεδομένα εντός του πραγματοποιούνται μόνο εμμέσως, προσθέτοντας δηλαδή νέα μπλοκ με τροποποιημένα δεδομένα, ενώ η διαγραφή των δεδομένων είναι αδύνατη. Επίσης, αν ο όγκος των συναλλαγών υπερβαίνει την ανωτέρω εκτίμηση, είναι αναμενόμενο να δημιουργηθούν προβλήματα. Συνεπώς, είναι σημαντικό να προηγηθεί εκτίμηση του μέγιστου αναμενόμενου όγκου συναλλαγών για την εκάστοτε περίπτωση, ώστε να αξιολογηθεί η καταλληλότητα της λύσης του BC.

Οργανώνοντας περαιτέρω τους ανωτέρω παράγοντες είναι εφικτό να σχεδιαστεί ένα δέντρο απόφασης, το οποίο θα μπορούσε να αξιοποιηθεί για την λήψη απόφασης σχετικά με την καταλληλότητα ή μη της τεχνολογίας BC για μια δεδομένη εφαρμογή:



Εικόνα 07: Δέντρο Απόφασης για την υιοθέτηση Blockchain

4.3.2. Σαφήνεια στην ανάλυση του πεδίου του έργου

Περαιτέρω, υφίσταται ανάγκη σαφούς προσδιορισμού των αναγκών, της υλοποίησης, των συμμετεχόντων και της αναμενόμενης αξίας για κάθε έναν από αυτούς. Σε αντίθεση, μια προσέγγιση του τύπου "ας βάλουμε όλα τα δεδομένα μας στο blockchain και θα σκεφτούμε αργότερα πώς θα τα χρησιμοποιήσουμε" είναι σίγουρο ότι θα αποτύχει για διάφορους λόγους, όπως για παράδειγμα, λόγω δυσκολίας εκτίμησης του όγκου των συναλλαγών και της ικανότητας του συστήματος να ανταπεξέλθει ή λόγω αποτυχίας να ληφθούν υπόψη ζητήματα ιδιωτικότητας και προστασίας δεδομένων κ.ο.κ. (Houlding, 2017)

4.3.3. Κοινωνικοί και Πολιτισμικοί παράγοντες

Επίσης, υφίστανται κρίσιμοι παράγοντες επιτυχίας που σχετίζονται με το γενικότερο κοινωνικό και πολιτισμικό πλαίσιο που παρατηρείται σε μια κοινωνία. Σύμφωνα με την Infosys (Infosys, 2017), μερικοί από τους κρισιμότερους σχετικούς παράγοντες είναι οι εξής:

- Εξοικείωση με την τεχνολογία

Το BC είναι από μόνο του αρκετά περίπλοκη έννοια, πόσο μάλλον αν μια κοινωνία δεν είναι εξοικειωμένη σε ικανοποιητικό βαθμό με τις νέες τεχνολογίες και δεν κατανοεί την αξία που αυτές μπορούν να προσδώσουν. Πολλές κοινωνίες, είτε για πολιτισμικούς λόγους, είτε λόγω αστοχιών του εκπαιδευτικού συστήματος, ή και λόγω έλλειψης τεχνολογικών δομών ή γενικότερης υποστήριξης, αντιμετωπίζουν τις νέες τεχνολογίες με επιφυλακτικότητα. Σε αυτές τις κοινωνίες η ευρεία υιοθέτηση τεχνολογιών BC φαντάζει πραγματικά απίθανη.

- Εξοικείωση με μη φυσικό χρήμα

Οι οικονομίες στις οποίες κυριαρχεί το ηλεκτρονικό χρήμα, οι κάρτες και οι ηλεκτρονικές πληρωμές, έναντι του φυσικού χρήματος και των μετρητών, έχουν να επωφεληθούν σαφώς περισσότερο από την τεχνολογία BC, η οποία θα προσδώσει νέα δυναμική σε αυτή την ήδη στέρεα βάση, στην οποία έχει εδραιωθεί μια κουλτούρα συναλλαγών με ηλεκτρονικό χρήμα.

- Μικρή συγκέντρωση ισχύος

Το BC δημιουργεί ένα σύστημα όπου κανένας μεμονωμένος χρήστης ή οργανισμός δεν έχει την δυνατότητα ελέγχου αυτού που συμβαίνει στο BC. Οι κοινωνίες, όπου παρατηρείται μικρότερη συγκέντρωση εξουσίας και πιο ισορροπημένες δυναμικές και όπου δεν υπάρχουν λίγες ισχυρές οντότητες, βαθιά περιχαρακωμένες στο σύστημα και στις διαδικασίες, είναι περισσότερο έτοιμες στην προοπτική ενός τέτοιου σεναρίου.

5. Εφαρμογές στη Δημόσια Διοίκηση

5.1. Ευρωπαϊκό επίπεδο

Τα οφέλη της τεχνολογίας BC έχουν προκαλέσει ήδη αυξημένο ενδιαφέρον σε μεγάλο αριθμό δημόσιων οργανισμών παγκοσμίως και αρκετοί από αυτούς έχουν αρχίσει να πειραματίζονται και να αναπτύσσουν πιλοτικά έργα.

Εικόνα 08: Καταγεγραμμένα έργα στο δημόσιο τομέα (μέχρι τον Μάρτιο του 2017.
Πηγή: Deloitte University Press

Πλέον, πάνω από 12 κυβερνήσεις, μεταξύ των οποίων του Καναδά, των ΗΠΑ, της Κίνας, της Ινδίας κ.α. αναπτύσσουν σχετικά έργα, είτε για να ελέγξουν την καταλληλότητα της τεχνολογίας, ως βάση για την παροχή δημόσιων υπηρεσιών προς τους πολίτες, είτε για να αναπτύξουν εσωτερικές εφαρμογές για την ίδια τη Δημόσια Διοίκηση (White & Killmeyer,

2017). Στη δεύτερη περίπτωση, μελετάται κυρίως η δυνατότητα ανάπτυξης ιδιωτικών και κοινοπρακτικών blockchains, καθώς ενέχουν μειωμένη πολυπλοκότητα -σε σχέση με τα δημόσια- και η εμπιστοσύνη σε αυτά εδράζεται σε νομικές συμφωνίες, αντί σε κρυπτο-οικονομικά κίνητρα.

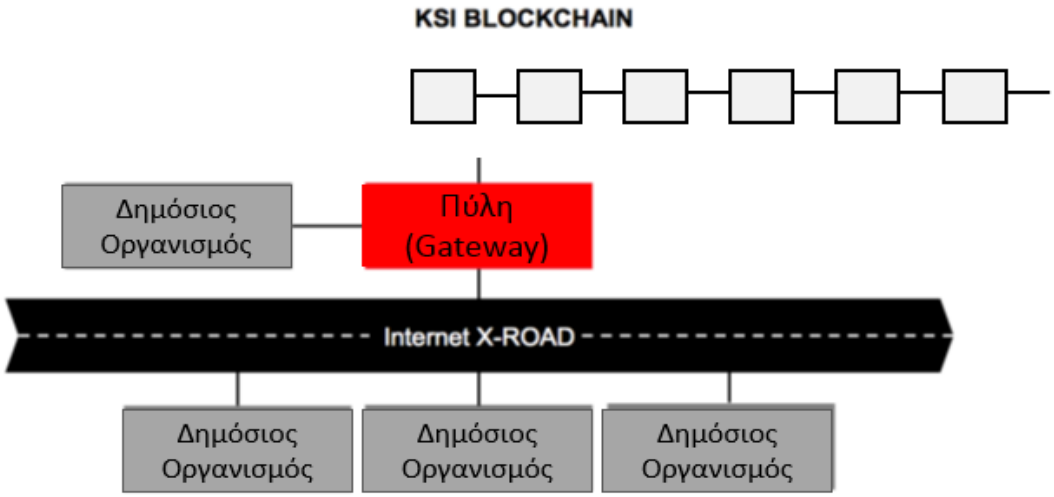
Σε ευρωπαϊκό επίπεδο οι δύο πιο σημαντικές εφαρμογές παρατηρούνται, αφενός, στην Σουηδία, όπου ένα ιδιωτικό BC χρησιμοποιείται από το εθνικό κτηματολόγιο (Lantmäteriet) ως πλατφόρμα για τις συναλλαγές στην ακίνητη περιουσία, σε συνεργασία με τη Σουηδική start-up Chromaway. Ο στόχος σε αυτή τη περίπτωση είναι η δραστική μείωση του απαραίτητου χρόνου για την ολοκλήρωση μιας αγοραπωλησίας ακινήτου, από 3-6 μήνες σε μερικές ώρες (Lantmäteriet, 2016). Αφετέρου, στην Εσθονία, η οποία γενικότερα αποτελεί μια από τις πιο προηγμένες κοινωνίες της πληροφορίας και της οποίας η εφαρμογή του BC, σε συνεργασία με την εταιρεία παροχής εταιρικών λύσεων BC 'Guardtime', διαπερνά όλη τη Δημόσια Διοίκηση. Για αυτόν ακριβώς τον λόγο αξίζει να γίνει μια πιο εκτεταμένη αναφορά σε αυτή την περίπτωση.

Στην εφαρμογή της Εσθονίας, που ονομάζεται Keyless Signature Infrastructure (KSI), το BC διαπερνά όλες τις σημαντικές υπηρεσίες και μητρώα της Δημόσιας Διοίκησης, όπως το μητρώο επιχειρήσεων, το κτηματολόγιο, τα δικαστικά αρχεία, τα αρχεία της αστυνομίας και το ηλεκτρονικό σύστημα υγείας, μέσω του X-Road. Το X-Road είναι μια πλατφόρμα διαλειτουργικότητας στην οποία είναι συνδεδεμένοι όλοι οι δημόσιοι φορείς στην Εσθονία[44]και η οποία υπηρετεί ως το κύριο κανάλι επικοινωνίας μεταξύ τους, υποστηρίζοντας την εγγραφή και την εύρεση σε πολλαπλές βάσεις δεδομένων, καθώς και την αντιγραφή και μεταφορά μεγάλων συνόλων δεδομένων. Όμως το X-Road δεν μπορεί να προστατέψει από μόνο του αποτελεσματικά έναν τόσο διάσπαρτο και μεγάλο όγκο δεδομένων, καθώς υπάρχουν πολλοί αστάθμητοι παράγοντες που μπορούν να τα τροποποιήσουν.

Σε αυτό το πλαίσιο, ο στόχος της εφαρμογής του BC είναι απλός: να εξαλειφθεί ο ανθρώπινος παράγοντας από την διαδικασία επιβεβαίωσης της ακεραιότητας των ψηφιακών δεδομένων (Guardtime, 2018). Ουσιαστικά, το KSI αξιοποιείται ως ένας μηχανισμός παροχής υπηρεσιών ψηφιακής υπογραφής. Ο χρήστης εκπέμπει στο δίκτυο το hash ενός στοιχείου και σε απάντηση παραλαμβάνει ένα token, το οποίο αποδεικνύει την συναλλαγή του. Το ίδιο τα στοιχείο παραμένει στον χρήστη και μόνο το hash αποστέλλεται στο KSI. Αυτός ο μηχανισμός αποδεικνύει την ύπαρξη της συναλλαγής, του χρόνου της συναλλαγής και την ιδιοκτησία του στοιχείου από τον συγκεκριμένο χρήστη. Παράλληλα, επιτρέπει την ανεξάρτητη - από τρίτους

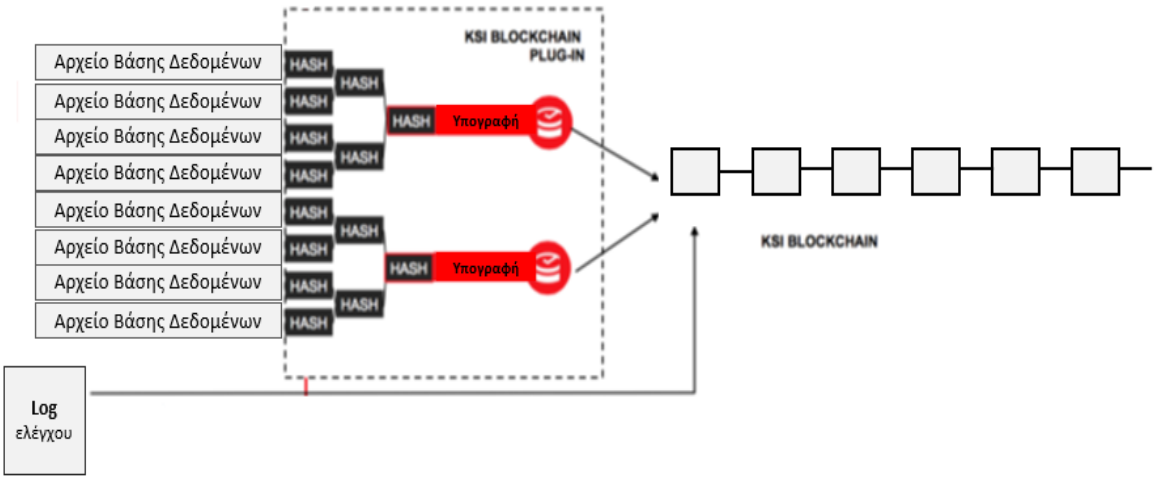
[44] Πάνω από 900 δημόσιοι οργανισμοί αξιοποιούν άμεσα το X-Road καθημερινά

- επαλήθευση των δεδομένων. (Martinovic, n.d). Στην εικόνα αποτυπώνεται ο τρόπος που ενσωματώνεται το KSI στις κυβερνητικές υπηρεσίες και ιδιαίτερα στη πλατφόρμα X-Road:



Εικόνα 09: Τρόπος ενσωμάτωσης του KSI στις κυβερνητικές υπηρεσίες

Στην επόμενη εικόνα αποτυπώνεται ο τρόπος που διασφαλίζει το KSI τα δεδομένα και τα αρχεία log στις βάσεις δεδομένων, σε ένα σύστημα βάσεων δεδομένων.



Εικόνα 10: Τρόπος διασφάλισης των δεδομένων και των αρχείων log σε ένα σύστημα ΒΔ από το KSI

Σε αυτό το σύστημα, ένα log αρχείο που εμπεριέχει τα στοιχεία του χρόνου, του χρήστη, των ρυθμίσεων και των στοιχείων που τυχόν τροποποιήθηκαν κ.α, εγγράφεται στο blockchain του KSI μαζί με τα hash των ίδιων των αρχείων. Αυτό το σύστημα εγγυάται ότι κάθε

τροποποίηση στο αρχείο μιας βάσης δεδομένων καταγράφεται και συνεπώς, διασφαλίζεται η ακεραιότητα της βάσης δεδομένων, ενώ παράλληλα, οι αλλαγές στα δεδομένα μπορούν να επαληθευτούν από τα αρχεία log, που με τη σειρά τους, επίσης προστατεύονται από το BC.

5.2. Εθνικό επίπεδο

5.2.1. Σχέση με την ηλεκτρονική διακυβέρνηση

Τις τελευταίες δύο δεκαετίες το κράτος δέχεται ισχυρές πιέσεις να βελτιώσει τις υπηρεσίες του και να μειώσει το κόστος λειτουργίας του για τους πολίτες. Στο πλαίσιο αυτό και σε συνδυασμό με τις τεχνολογικές εξελίξεις αναδύθηκε η έννοια της ηλεκτρονικής διακυβέρνησης, ως μια προσπάθεια ενίσχυσης της αποτελεσματικότητας και μείωσης του λειτουργικού κόστους του δημοσίου. Σήμερα, η στρατηγική για την ηλεκτρονική διακυβέρνηση της χώρας εντάσσεται στην Εθνική Ψηφιακή Στρατηγική (ΕΨΣ) 2016-2021 (Γενική Γραμματεία Ψηφιακής Πολιτικής, 2016), που δημοσιεύτηκε το Δεκέμβρη του 2016 από τη Γενική Γραμματεία Ψηφιακής Πολιτικής (ΓΓΨΠ). Η ΓΓΨΠ είχε ιδρυθεί λίγους μήνες νωρίτερα, για να αποτελέσει μία κεντρική δομή, υπεύθυνη για τον κεντρικό σχεδιασμό, συντονισμό και παρακολούθηση της υλοποίησης έργων ΤΠΕ στο ελληνικό δημόσιο και στη χώρα συνολικά.

Στην ΕΨΣ ορίζονται επτά (7) τομείς παρέμβασης και οι εκάστοτε προτεραιότητες για τον καθένα από αυτούς με αντίστοιχη πρόβλεψη δράσεων. Ο 5ος τομέας («Ριζική αναθεώρηση του τρόπου παροχής Ψηφιακών Υπηρεσιών του Δημοσίου») εστιάζει κατ' ουσίαν στην ηλεκτρονική διακυβέρνηση και είναι ο άξονας στον οποίο μπορούν λογικά να ενταχθούν έργα που αφορούν την παροχή υπηρεσιών με τεχνολογία BC, καθώς ιδιαίτερα στο πλαίσιο της Προτεραιότητας 5.4 (Επιβολή της διαλειτουργικότητας) και της Προτεραιότητας 5.5 (Βελτίωση των δημόσιων μητρώων και των ανοικτών δεδομένων) του 5^{ου} τομέα, υπάρχουν τα νομιμοποιητικά ερείσματα που ευνοούν την ανάπτυξη εφαρμογών BC. Εξετάζοντας όμως τα ολοκληρωμένα ή υπό εξέλιξη έργα στον κλάδο ΤΠΕ, εξάγεται το συμπέρασμα ότι μέχρι πρόσφατα, σε αυτά δεν περιλαμβάνονταν έργα που αξιοποιούν την τεχνολογία BC,[45] παρόλο

[45] Για ένα πληρέστερο κατάλογο ή για αναζήτηση έργων που έχουν δρομολογηθεί ή υλοποιηθεί, ο αναγνώστης μπορεί να ανατρέξει στην ιστοσελίδα του Ε.Π. «Ψηφιακή Σύγκλιση», όπου συμπεριλαμβάνονται όσα έργα εντάσσονται σε αυτό το Επιχειρησιακό Πρόγραμμα και του Ε.Π. «Διοικητική Μεταρρύθμιση».

που η ΕΕ, όπως έχει αναφερθεί σε προηγούμενο κεφάλαιο, χρηματοδοτεί σχετικά έργα μέσω του FP7 και του Horizon2020, ήδη από το 2013.

5.2.2. Έργα blockchain υπό το Horizon 2020

Πλέον όμως, κάτω από τη Πρόσκληση του Horizon 2020 με τίτλο 'Socioeconomic and cultural Transformations in the Context of the 4th Industrial Revolution', που εμπεριέχει τον άξονα 'Transformative impact of disruptive technologies in public services', έχει εγκριθεί για χρηματοδότηση για τη περίοδο 2019-2021 ένα έργο με τίτλο 'Decentralised Qualifications, Verification and Management for Learner Empowerment, Education Reengineering and Public Sector Transformation', με συντονιστή το Εθνικό Μετσόβιο Πολυτεχνείο και πολλούς άλλους συμμετέχοντες φορείς, μεταξύ των οποίων είναι το ΑΣΕΠ. Αν και οι τεχνικές λεπτομέρειες δεν είναι ακόμα γνωστές, ο στόχος είναι να αξιοποιηθεί η τεχνολογία BC ως πλατφόρμα για την αποθήκευση, τον διαμοιρασμό και την επαλήθευση της ακεραιότητας των εκπαιδευτικών και επαγγελματικών προσόντων. (European Commission, CORDIS, 2018)

5.2.3. Άλλες δράσεις

- Διοργάνωση θεματικών Hackathlons

Στην ΕΨΣ προβλέπεται, μεταξύ άλλων, η ριζική αναθεώρηση και ο εκσυγχρονισμός του τρόπου υλοποίησης των έργων ΤΠΕ, ώστε να διευκολύνεται η συμμετοχή μικρών και μεσαίων επιχειρήσεων, διευρύνοντας τη βάση προμηθευτών του Δημοσίου. Οι σχετικές παρεμβάσεις περιλαμβάνουν, μεταξύ άλλων, τη τακτική διοργάνωση ή υποστήριξη θεματικών hackathons, ώστε να έχουν την ευκαιρία καινοτόμες ομάδες και νεοφυείς επιχειρήσεις να σχεδιάσουν και να προσφέρουν καινοτόμες λύσεις ΤΠΕ στο ελληνικό δημόσιο.

Στον πλαίσιο αυτό, υπό την αιγίδα του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών & Ενημέρωσης διοργανώθηκε από τις 28 Ιουνίου έως την 1η Ιουλίου του 2018, ο 2ος Μαραθώνιος Καινοτομίας για εφαρμογές έξυπνων πόλεων. Στη διοργάνωση συμμετείχαν 128 ομάδες νέων και πάνω από 400 διαγωνιζόμενοι. Ιδιαίτερο ενδιαφέρον έχει το γεγονός ότι το 1ο βραβείο απονεμήθηκε στην ομάδα «No code scheduled» για μια λύση που

φιλοδοξεί να ελαχιστοποιήσει τις ουρές στις δημόσιες υπηρεσίες και στηρίζεται στην τεχνολογία blockchain (Γενική Γραμματεία Ψηφιακής Πολιτικής, 2018).

- Ευρωπαϊκή Εταιρική Σχέση Blockchain (European Blockchain Partnership, EBP)

Στις 23 Μαΐου του 2018 η Ελλάδα υπέγραψε την κοινή δήλωση για τη δημιουργία της Ευρωπαϊκής Εταιρικής Σχέσης Blockchain, με την οποία 25 συνολικά κράτη μέλη της ΕΕ και η Νορβηγία συμφώνησαν να συνεργαστούν για τη δημιουργία μιας Ευρωπαϊκής Υποδομής Υπηρεσιών Blockchain (EBSI), η οποία θα υποστηρίζει την παροχή διασυνοριακών ψηφιακών δημόσιων υπηρεσιών. Σύμφωνα με την κοινή αυτή δήλωση, η στενή συνεργασία θα συμβάλλει στην αποφυγή αποσπασματικών προσεγγίσεων και θα εξασφαλίσει τη διαλειτουργικότητα και την ευρύτερη ανάπτυξη υπηρεσιών βασισμένων στο BC. (European Commission, 2018)

- Υπογραφή της Διυπουργικής Διακήρυξης χωρών της Ν. Ευρώπης για τις Τεχνολογίες Κατανεμημένου Καθολικού

Ο Γενικός Γραμματέας Ψηφιακής Πολιτικής συμμετείχε στις εργασίες του Ευρωπαϊκού Συμβουλίου Τηλεπικοινωνιών της 4ης Δεκεμβρίου 2018, στις Βρυξέλλες. Στο περιθώριο του Συμβουλίου, συναντήθηκε με τους υπόλοιπους έξι εταίρους του της ομάδας Med7 (Κύπρος, Γαλλία, Ιταλία, Μάλτα, Πορτογαλία, Ισπανία) για την υπογραφή της Διυπουργικής Διακήρυξης για τις Τεχνολογίες Κατανεμημένου Καθολικού**.** Πρόκειται για μια κίνηση των κρατών μελών του ευρωπαϊκού Νότου που σηματοδοτεί τη δέσμευση των Μεσογειακών χωρών να συνεργαστούν για να διεκδικήσουν ηγετικό ρόλο στην ανάπτυξη νέων τεχνολογιών. (Υπουργείο Ψηφιακής Πολιτικής, 2018)

- Hellenic Blockchain Hub

Τέλος, σε επίπεδο Κοινωνίας των Πολιτών, αξίζει να αναφερθεί το 'Hellenic blockchain Hub'[46], το οποίο είναι ένα υπό διαμόρφωση ακόμα, μη κερδοσκοπικό δίκτυο στελεχών από το δημόσιο και τον ιδιωτικό τομέα, με ενδιαφέρον και διάθεση να προωθήσουν τη γνώση γύρω από την τεχνολογία blockchain – DLT.

[46] Βλ. http://blockchain.org.gr/home/

6. Πρόταση εφαρμογής στην ελληνική Δημόσια Διοίκηση

6.1. Εφαρμογή στο πεδίο της διαχείρισης του ανθρώπινου δυναμικού, στο στάδιο της επιλογής και πρόσληψης του προσωπικού

Λαμβάνοντας υπόψη την ανωτέρω ανάλυση, είναι προφανές ότι η τεχνολογία BC θα μπορούσε να αποδειχθεί ιδιαίτερα χρήσιμη στη Δημόσια Διοίκηση, σε μια σειρά από πεδία στα οποία θα μπορούσαν να αξιοποιηθούν οι εγγενείς δυνατότητες της, δηλαδή η δυνατότητα απόδειξης της ύπαρξης (Proof of Existence), του χρόνου (Proof of Time) και της ιδιοκτησίας (Proof of Ownership) ενός ψηφιακού στοιχείου. Στο πλαίσιο αυτό, μια πρόταση που ικανοποιεί παράλληλα και όλα τα κριτήρια στο προαναφερθέν «δέντρο απόφασης», είναι η εφαρμογή της τεχνολογίας BC στο πεδίο της διαχείρισης του ανθρώπινου δυναμικού και συγκεκριμένα, στο στάδιο της επιλογής και πρόσληψης του προσωπικού του.

6.1.1. Το πρόβλημα

Ένας από τους βασικούς θεσμικούς εγγυητές της τήρησης των αρχών της διαφάνειας, της αντικειμενικότητας και της αξιοκρατίας στην επιλογή του προσωπικού του δημόσιου τομέα είναι το Ανώτατο Συμβούλιο Επιλογής Προσωπικού (ΑΣΕΠ), το οποίο συστάθηκε με το Ν. 2190/1994[47] ως ανεξάρτητη αρχή. Στις βασικές αρμοδιότητες του περιλαμβάνεται η επιλογή του τακτικού προσωπικού του δημόσιου και ευρύτερου δημόσιου τομέα, και ο έλεγχος της νομιμότητας των διαδικασιών πρόσληψης του προσωπικού (ΕΚΔΔΑ, 2018). Στο πλαίσιο αυτό και ανάλογα με τον ετήσιο σχεδιασμό των δημόσιων υπηρεσιών, το ΑΣΕΠ οργανώνει τη διαδικασία επιλογής του προσωπικού, η οποία διαφοροποιείται ανάλογα με τη κατηγορία του (άρθ. 17, 18, 19 του ν.2190).

Σε κάθε περίπτωση όμως, ο έλεγχος των τυπικών προσόντων των συμμετεχόντων στις διαδικασίες πραγματοποιείται από το προσωπικό του ΑΣΕΠ και γίνεται πάντα με ομοιόμορφο τρόπο, δηλαδή, οπτικός έλεγχος των δικαιολογητικών, βάσει των απαιτήσεων της προκήρυξης

[47] ΦΕΚ 28/Α/3-3-1994 (Σύσταση ανεξάρτητης αρχής για την επιλογή προσωπικού και ρύθμιση θεμάτων διοίκησης)

και επικοινωνία με τον εκδότη ενός πιστοποιητικού, σε περίπτωση υπόνοιας παραποίησης ή ψευδούς περιεχομένου. Αυτή η διαδικασία είναι επιρρεπής, τόσο σε σφάλματα από αμέλεια, όσο και σε κακόβουλες παρεμβάσεις και ασφαλώς δεν ικανοποιεί στο έπακρο τις απαιτήσεις ενός ποιοτικού ελέγχου. Τέλος, απαιτεί πολύ χρόνο και παρουσιάζει υψηλό κόστος, λόγω της μεγάλης κλίμακας των απαραίτητων ανθρωποωρών για τη διενέργεια της διαδικασίας ελέγχου. Δεδομένου του μεγάλου όγκου προκηρύξεων που διαχειρίζεται το ΑΣΕΠ και του μικρού αριθμού του προσωπικού του, αυτό οδηγεί περαιτέρω σε συμφόρηση της διαδικασίας, σε καθυστερήσεις στην ολοκλήρωση των διαγωνισμών και σε καθυστερημένη επάνδρωση των υπηρεσιών με το απαραίτητο προσωπικό, με πολλαπλές αρνητικές επιπτώσεις.

Στο δεύτερο σκέλος, την πρόσληψη του προσωπικού στους φορείς της Δημόσιας Διοίκησης, δηλαδή στη περίοδο πριν την υπογραφή της πράξεως διορισμού, σύμφωνα με το άρθρο 28 του ν. 4305/2014[48], οι υπηρεσίες είναι υποχρεωμένες να διενεργούν αμελλητί, υποχρεωτικά αυτεπάγγελτο έλεγχο της γνησιότητας των δικαιολογητικών που έχει υποβάλει ο υποψήφιος και που είναι απαραίτητα για το διορισμό/πρόσληψή του. Για το σκοπό αυτό οι υπηρεσίες αποστέλλουν στους αρμόδιους φορείς με τηλεομοιότυπο (fax) ή με ηλεκτρονικό ταχυδρομείο αντίγραφα των τίτλων των υποψηφίων για τη διαπίστωση της γνησιότητας τους.

Οι ανωτέρω διατάξεις, αν και αναγκαίες για τη διασφάλιση της ακεραιότητας και αυθεντικότητας των δικαιολογητικών που τεκμηριώνουν τον διορισμό και την ενίσχυση της αξιοκρατίας και της αντικειμενικότητας, εντούτοις, λόγω της αρχιτεκτονικής τους και του χειρωνακτικού τρόπου διενέργειάς τους δημιουργούν έναν υπέρογκο φόρτο εργασίας στις διευθύνσεις ανθρώπινου δυναμικού των φορέων και στα εκπαιδευτικά ιδρύματα, τους φορείς πιστοποίησης κ.α. που καλούνται να τεκμηριώσουν την εγκυρότητα των πιστοποιητικών. Αυτό μεταφράζεται σε υψηλό κόστος, μεγάλο χρόνο ολοκλήρωσης της διαδικασίας, σφάλματα, ευκαιρίες για κακόβουλες παρεμβάσεις και γενικότερα χαμηλή ποιότητα ελέγχου.

Παράλληλα, η έκδοση και η επικύρωση της ακεραιότητας των πιστοποιητικών (σπουδών, επαγγελματικών προσόντων κ.α.) συμβαίνει αποκλειστικά κάτω από την σκεπή κάποιου εκπαιδευτικού οργανισμού. Και παρά τις συνεχείς προσπάθειες ψηφιοποίησης των τελευταίων ετών, οι περισσότεροι εκπαιδευτικοί οργανισμοί και φορείς στη χώρα μας έχουν υιοθετήσει ένα υβριδικό σύστημα έκδοσης βεβαιώσεων, όπου συνδυάζουν την έκδοση των βεβαιώσεων σε έντυπη μορφή, το οποίο παραδίδουν στον αποδέκτη, με ένα αντίγραφο

[48] ΦΕΚ 237/Α/31.10.2014 (Ανοικτή διάθεση και περαιτέρω χρήση εγγράφων, πληροφοριών και δεδομένων του δημόσιου τομέα)

ασφαλείας, ψηφιοποιημένο στη κεντρική βάση δεδομένων τους. Αυτό το σύστημα, όμως, έχει τους εξής περιορισμούς:

- η δυνατότητα πλαστογράφησης, τόσο των έντυπων, όσο και των ηλεκτρονικών πιστοποιητικών (χωρίς ψηφιακή υπογραφή),
- οι οργανισμοί που εκδίδουν τα πιστοποιητικά αποτελούν ένα μοναδικό σημείο αστοχίας, ενώ η ασφαλής διατήρησή τους σε πολλαπλά αντίγραφα απαιτεί κοστοβόρα και πολύπλοκα συστήματα, επιρρεπή σε αστοχίες,
- η πιθανότητα κακόβουλης αλλοίωσης από προσωπικό του ίδιου του φορέα έκδοσης,
- η διατήρηση ενός μητρώου και η απάντηση στα ερωτήματα από τους ενδιαφερόμενους αποτελεί μια χειρωνακτική διαδικασία, με αυξημένο κόστος και ανάγκες σε ανθρωποώρες.
- είναι επιρρεπή σε ηλεκτρονικές επιθέσεις

6.1.2. Η πρόταση

Σε αυτό το πλαίσιο, προτείνεται μια νέα αρχιτεκτονική βασισμένη στο BC, η οποία θα επιτρέψει ουσιαστικά δύο συνθήκες:

1. Την δυνατότητα αυθεντικοποίησης και επαλήθευσης της ακεραιότητας ενός πιστοποιητικού, άμεσα, εύκολα και χωρίς την ανάγκη επικοινωνίας με τον φορέα έκδοσής του.
2. Την δυνατότητα αυθεντικοποίησης και επαλήθευσης της ακεραιότητας ενός πιστοποιητικού, ακόμα και στη περίπτωση που ο φορέας έκδοσης του έχει πάψει να υφίσταται.

Η πρόταση αφορά την μετάπτωση από το σημερινό συγκεντρωτικό σύστημα αυθεντικοποίησης και επαλήθευσης της ακεραιότητας των πιστοποιητικών, προς μια τεχνολογία κατανεμημένου καθολικού, το οποίο θα είναι διαμοιρασμένο και συγχρονισμένο προς επικύρωση σε ένα P2P δίκτυο, στο οποίο ενδεικτικά θα συμμετέχουν οι εξής φορείς:

- ΑΕΙ/ΤΕΙ
- Φορείς Πιστοποίησης Γνώσεων (πχ. ECDL)
- Επαγγελματικά Επιμελητήρια
- ΑΣΕΠ

Σε αυτό το σενάριο, οι εκπαιδευτικοί οργανισμοί που εκδίδουν πιστοποιητικά και οι υπόλοιποι ενδιαφερόμενοι φορείς θα σχηματίσουν ένα κοινοπρακτικό BC με άδειες πρόσβασης. Η προσέγγιση που θα ακολουθηθεί προτείνεται να είναι:

α) Είτε η BaaS, σε συνεργασία με κάποια από τις μεγάλες εταιρείες (IBM, Microsoft) καθώς η συγκεκριμένη προσέγγιση υπερσκελίζει το πρόβλημα της διαμόρφωσης και ρύθμισης του πολύπλοκου λειτουργικού περιβάλλοντος που απαιτείται. Επίσης, με αυτήν την μέθοδο δεν θα χρειαστεί οι φορείς να προβούν σε επενδύσεις σε εξοπλισμό.

β) Είτε μια κάθετη -κλαδική- λύση, όπου η πρόσβαση των συμμετεχόντων/κόμβων στο BC θα διενεργείται μέσω ενός API, που θα 'κρύβει' την επικοινωνία με το BC και θα επιτρέπει τη διαχείριση του συστήματος μέσω ενός πολύ απλούστερου web interface, για διευκόλυνση της διαλειτουργικότητας.

Ανεξαρτήτως προσέγγισης, σε αυτό το δίκτυο οι υπεύθυνοι επικύρωσης των μπλοκ θα είναι όλοι οι συμμετέχοντες, με ίσα δικαιώματα στη διαδικασία συναίνεσης. Το κίνητρο για την παροχή της επεξεργαστικής τους ισχύος δεν θα στηρίζεται σε κάποιο κρυπτονόμισμα, αλλά θα συμμετέχουν στο δίκτυο γιατί ανήκουν στους άμεσα ενδιαφερόμενους και αποκομίζουν οφέλη από τη γενικότερη επιχειρησιακή λειτουργία τους, όπως μειωμένο διοικητικό κόστος, ευκολία, αυξημένο κύρος βεβαιώσεων σπουδών κ.α. Η εμπιστοσύνη μεταξύ τους, θα παρέχεται από διμερείς ή πολυμερείς νομικές συμφωνίες μεταξύ των φορέων, όπως συνηθίζεται στα κοινοπρακτικά BC. Τα δικαιώματα ανάγνωσης θα είναι δημόσια για να έχουν πρόσβαση οι αποδέκτες των πιστοποιητικών και για να διασφαλίζεται υψηλός βαθμός διαφάνειας.

Για λόγους συμμόρφωσης με τη νομοθεσία για τα προσωπικά δεδομένα, θα ακολουθηθεί η προσέγγιση που έχει αναλυθεί στο κεφάλαιο με τις νομικές πτυχές του BC, δηλαδή, στο δίκτυο αυτό θα αποθηκεύονται μόνο τα κρυπτογραφικά hash των ψηφιακών πιστοποιητικών που εκδίδονται από τους φορείς, ενώ τα πρωτότυπα πιστοποιητικά και τυχόν προσωπικά δεδομένα θα διατηρούνται στις ΒΔ των φορέων και φυσικά θα παρέχονται και στους ίδιους τους αποδέκτες. Σε ένα τέτοιο πλαίσιο, η αυθεντικοποίηση ενός πιστοποιητικού θα απαιτεί μόνο την σύγκριση με το hash που βρίσκεται αποθηκευμένο στο BC.

6.1.3. Αρχιτεκτονική της εφαρμογής

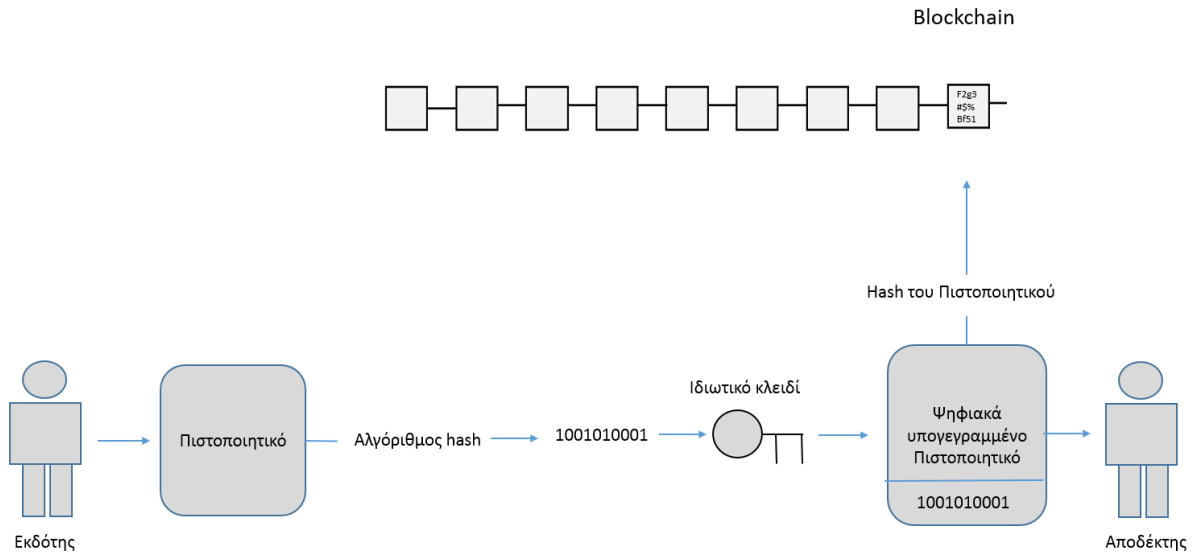
Στην πιο απλή μορφή, μία πιστοποίηση (σπουδών, επαγγελματικών προσόντων κ.α.) είναι η έκδοση μιας βεβαίωσης που πιστοποιεί ότι ισχύει μια σειρά από συνθήκες. Από τη στιγμή που ένα πιστοποιητικό αποτελεί μια έκδοση βεβαίωσης από ένα μέρος σε ένα άλλο,

είναι πολύ σημαντικό για την καθιέρωση μιας σχέσης εμπιστοσύνης, να ισχύουν τουλάχιστον τρεις προϋποθέσεις (Grech & Camilleri, 2017):

- να υπάρχει η δυνατότητα επαλήθευσης της ταυτότητας τόσο του εκδότη, όσο και του αποδέκτη
- να υφίσταται η βεβαιότητα ότι το πιστοποιητικό δεν είναι προϊόν πλαστογραφίας
- Να υφίσταται εύκολη πρόσβαση σε αυτό

Στο πλαίσιο αυτό, η τεχνολογία BC είναι ιδανική ως υποδομή διασφάλισης και αυθεντικοποίησης των εκπαιδευτικών προσόντων, καθώς έχει τη δυνατότητα να αποθηκεύει μια λίστα με τον εκδότη και τον αποδέκτη κάθε πιστοποιητικού, μαζί με την σύνοψη της ψηφιακής υπογραφής κάθε εγγράφου (hash), σε μια κοινή, αποκεντρωμένη και κατανεμημένη βάση δεδομένων, στην οποία η πρόσβαση είναι εύκολη στους συμμετέχοντες. Η διαδικασία αυτή ακολουθεί τα εξής βήματα:

1. Ο εκδότης του πιστοποιητικού δημιουργεί ένα ψηφιακό αρχείο που περιέχει βασικές πληροφορίες, όπως την ονομασία του εκδότη και του αποδέκτη, την ημερομηνία, την πιστοποίηση κ.α.
2. Ο εκδότης δημιουργεί το κρυπτογραφικό hash του αρχείου με έναν hash generator
3. Ο εκδότης υπογράφει ψηφιακά με το ιδιωτικό του κλειδί το αρχείο.
4. Ο εκδότης χρησιμοποιεί το ιδιωτικό του κλειδί για να δημιουργήσει μια συναλλαγή στο BC, μεταξύ της διεύθυνσης του και της διεύθυνσης του συγκεκριμένου αποδέκτη του πιστοποιητικού.



Εικόνα 11: Δημοσίευση ενός πιστοποιητικού στο Blockchain

Με αυτόν τον τρόπο, τα δεδομένα που είναι απαραίτητα για την επαλήθευση της ακεραιότητας και της αυθεντικότητας ενός πιστοποιητικού βρίσκονται ασφαλώς αποθηκευμένα για πάντα στο BC, ακόμα και αν ο φορέας πιστοποίησης πάψει να υπάρχει. Για να επαληθεύσει κάποιος ενδιαφερόμενος (δημόσιος ή ιδιωτικός εργοδότης ή κάποια αρχή, πχ. ΑΣΕΠ) το πιστοποιητικό, αρκεί να ακολουθήσει την ανωτέρω διαδικασία με την ανάποδη φορά, ώστε να επιβεβαιώσει ότι το hash αντιστοιχεί στο πρωτότυπο αρχείο και ότι τα κλειδιά ανήκουν στο σωστό οργανισμό.

Η αποθήκευση των ίδιων των πρωτότυπων πιστοποιητικών και άλλων μεταδεδομένων θα πραγματοποιείται, αφενός στην κεντρική βάση δεδομένων του εκδότη, αφετέρου σε μέσο αποθήκευσης (πχ. σκληρός δίσκος, ψηφιακό πορτοφόλι κ.α.) του αποδέκτη του πιστοποιητικού, από το οποίο θα μπορεί εύκολα αυτός να τα διαμοιραστεί με τρίτους ή ακόμα και να τα εκτυπώσει.

6.1.4. Προστιθέμενη αξία της εφαρμογής

Ο βασικός στόχος της μετάπτωσης σε αυτό το σύστημα είναι ο μετασχηματισμός του πιστοποιητικού, από κάτι το οποίο λαμβάνει αποκλειστικά ο ίδιος ο ωφελούμενος της εκπαιδευτικής διαδικασίας, σε ένα αυτόματα επαληθεύσιμο στοιχείο πληροφορίας, στο οποίο μπορεί να αποκτήσει πρόσβαση κάποιος ενδιαφερόμενος, με αδιάβλητο τρόπο, χωρίς την εξάρτηση από κάποια κεντρική οντότητα.

Στο πλαίσιο αυτό, αντικαθίσταται η κεντρική οντότητα με ένα πιο ανθεκτικό αποκεντρωμένο δίκτυο, που παρουσιάζει το πρόσθετο πλεονέκτημα ότι κανένας τρίτος δεν μπορεί να αλλοιώσει τα εγγεγραμμένα στα μπλοκ δεδομένα και συνεπώς, αυξάνεται κατακόρυφα το επίπεδο ασφάλειας και ακεραιότητας τους.

Επίσης, η επαλήθευση ενός πιστοποιητικού θα μπορεί να ολοκληρωθεί από οποιονδήποτε ενδιαφερόμενο έχει πρόσβαση στο δίκτυο, ακόμα και αν ο οργανισμός που το παρείχε έχει πάψει να υπάρχει. Επιπλέον, από τη στιγμή που ένας οργανισμός εκδώσει ένα πιστοποιητικό, δεν χρειάζεται να αφιερώσει επιπρόσθετους πόρους για να επιβεβαιώνει σε τρίτους την ισχύ του πιστοποιητικού, καθώς θα είναι σε θέση να επαληθεύσουν οι ίδιοι την αυθεντικότητά του στο BC.

Τέλος, το hash απλά αποτελεί ένα σύνδεσμο προς το πρωτότυπο αρχείο, το οποίο είναι υπό τον έλεγχο του χρήστη, προστατεύοντας με αυτόν τον τρόπο την ιδιωτικότητά του και καθιστώντας το σύστημα συμβατό με τη νομοθεσία για τα προσωπικά δεδομένα.

Αν και η συγκεκριμένη πρόταση δεν αποτελεί λύση σε όλα τα προβλήματα του κεντρικού τρόπου αποθήκευσης - και επαλήθευσης της ακεραιότητας των πιστοποιητικών - καθώς δεν αποφεύγονται τα μειονεκτήματα που εγκυμονούν στα κοινοπρακτικά blockchain, εντούτοις, πετυχαίνει να αντιμετωπίσει τα σημαντικότερα από αυτά και ασφαλώς, να πετύχει τον στόχο της αποσυμφόρησης της διαδικασίας επιλογής προσωπικού, της δραστικής μείωσης των απαραίτητων ανθρωποωρών για τη διενέργεια των απαραίτητων ελέγχων, τον εξορθολογισμό του κόστους και του χρόνου της όλης διαδικασίας και την δραστική αύξηση της ποιότητας και της εμπιστοσύνης στο σύστημα. Τέλος, δεν απαιτεί την δραστική αναμόρφωση της πληροφοριακής δομής των φορέων, καθώς ουσιαστικά θα διατηρήσουν τις κεντρικές βάσεις δεδομένων τους, ενώ δεν απαιτείται ο γνωστός ενεργοβόρος μηχανισμός συναίνεσης μεταξύ των συμμετεχόντων, λόγω της κοινοπρακτικής φύσης του δικτύου.

6.1.5. Σημαντικότερα εμπόδια

Παρόλα τα πλεονεκτήματα που παρουσιάζει η μετάπτωση στη τεχνολογία BC στο πεδίο της επαλήθευσης της ακεραιότητας και της αυθεντικοποίησης των πιστοποιητικών εκπαίδευσης, ασφαλώς παρουσιάζει και σημαντικά εμπόδια. Εκτός από τις προαναφερθείσες ιδιαίτερες αδυναμίες των κοινοπρακτικών blockchain, πρέπει να προστεθούν επιπλέον και τα εξής:

1. Υπάρχει το ζήτημα της ύπαρξης -ή μη- διάθεσης των εκπαιδευτικών οργανισμών να ανταλλάξουν τις απαραίτητες πληροφορίες, καθώς και της διάθεσης ή μη των υπόλοιπων ενδιαφερόμενων να επαληθεύσουν την ακεραιότητα των πιστοποιητικών, χωρίς να επικοινωνήσουν με τον εκπαιδευτικό οργανισμό. Τίθονται δηλαδή ζητήματα γενικότερης διοικητικής και οργανωσιακής κουλτούρας.

2. Σε σχέση και με το ανωτέρω ζήτημα, υφίσταται η ανάγκη να επικοινωνηθεί με σαφή και κατανοητό τρόπο η πολύπλοκη αυτή τεχνολογία και τα πλεονεκτήματά της - ιδιαίτερα στην ομάδα ενδιαφέροντος- ως απαραίτητη προϋπόθεση για μια προσπάθεια που επιδιώκει να έχει κάποιο βαθμό επιτυχίας.

7. Συμπεράσματα και Επίλογος

Παρά τις αναμφισβήτητες προς το παρόν αδυναμίες της τεχνολογίας ΒC, τις διάφορες φωνές που ακούγονται για την ανωριμότητα της τεχνολογίας και τις εκτιμήσεις για υπερβολικό, χωρίς αντίκρισμα, ενθουσιασμό, είναι γεγονός, ότι, παρατηρώντας τις κινήσεις των μεγάλων εταιρειών στον χώρο (IMB, Microsoft κ.α.) και τους πόρους που αυτές έχουν επενδύσει και συνεχίζουν να διαθέτουν για την ανάπτυξη της συγκεκριμένης τεχνολογίας, είναι εξαιρετικά δύσκολο να πιστέψει κάποιος ότι δεν υπάρχει τίποτα αξιόλογο σε αυτή. Αυτή η εντύπωση ενισχύεται, αν κανείς εξετάσει τα έργα ΒC που βρίσκονται σε εξέλιξη διεθνώς και αποτυπώσει την ανοδική τάση ανάπτυξής τους τα τελευταία χρόνια. Επίσης, σε αμιγώς ευρωπαϊκό επίπεδο, η εντύπωση αυτή ενδυναμώνεται ακόμα περισσότερο, αν ληφθούν υπόψη οι δηλώσεις και οι σχετικές δράσεις από την πλευρά της ίδιας της ΕΕ.

Αυτό που φαίνεται πάντως βέβαιο, είναι ότι οι όποιες λύσεις εφαρμοστούν, θα περιλαμβάνουν διάφορα είδη ΒC και όχι μία μόνο τεχνολογική υλοποίηση. Και αυτό, γιατί διαφορετικοί τομείς έχουν ανάγκη από διαφορετικά εργαλεία και μέχρι στιγμής δεν υφίσταται κάποιο πρωτόκολλο ΒC που να είναι κατάλληλο για όλους. Συνεπώς, σε κάποιες περιπτώσεις θα είναι προτιμότερο το δημόσιο ΒC, βασισμένο στο πρωτόκολλο bitcoin ή στο ethereum, ενώ σε άλλες, βέλτιστη επιλογή είναι πιθανό να αποτελεί ένα ΒC με άδειες πρόσβασης. Γι’ αυτόν ακριβώς τον λόγο είναι σημαντικό να κατανοηθεί, ότι αν και το παράδειγμα του bitcoin είναι χρήσιμο για να αναλυθεί και να γίνει κατανοητή η τεχνολογία ΒC, εντούτοις, δεν απαιτούν όλες οι υλοποιήσεις τις ιδιότητες και τα χαρακτηριστικά ενός δημόσιου ΒC.

Μία πτυχή που πρέπει οπωσδήποτε να ληφθεί σοβαρά υπόψη, πριν την επιλογή μιας συγκεκριμένης υλοποίησης, ιδιαίτερα μετά την θέσπιση και θέση σε ισχύ του ΓΚΠΔ, είναι το τί δεδομένα θα αποθηκεύονται στο ΒC. Η απάντηση μπορεί σε πολλές περιπτώσεις να είναι «όχι όλα». Είναι πολύ πιθανό -και τεχνικά υλοποιήσιμο- να πρέπει να αποθηκεύονται κάποια δεδομένα (προσωπικά, μεγάλου μεγέθους κ.α.) στις εξωτερικές ΒΔ των οργανισμών και να αποθηκεύεται μόνο η κρυπτογραφική τους σύνοψη στο ΒC. Μία τέτοια περίπτωση, άλλωστε, περιεγράφηκε και στην πρόταση εφαρμογής για την ελληνική Δημόσια Διοίκηση.

Σε κάθε περίπτωση, το σημαντικότερο για τη Δημόσια Διοίκηση σήμερα είναι, καταρχάς, να βρίσκεται σε συνεχή επαφή με τις τρέχουσες εξελίξεις γύρω από τη συγκεκριμένη τεχνολογία και να παρέχει σχετική εκπαίδευση στα στελέχη της. Αυτό, οφείλει να περιλαμβάνει μια συνειδητή προσπάθεια, όχι μόνο απλής ενημέρωσης, αλλά και αποκόμισης

σχετικής τεχνογνωσίας και ικανότητας υλοποίησης έργων. Προϋπόθεση βέβαια για αυτό, είναι να γίνουν πρώτα κατανοητά τα οφέλη, οι πραγματικές δυνατότητες, καθώς και οι περιορισμοί αυτής της τεχνολογίας. Σε αυτό το κομμάτι, η εργασία αυτή ευελπιστεί να έχει κάποια προστιθέμενη αξία.

Παράλληλα, η Πολιτεία οφείλει να αναγνωρίσει και να θεσπίσει το κατάλληλο κανονιστικό και ρυθμιστικό πλαίσιο, που αφενός, θα επιτρέψει στις επιχειρήσεις και τους ιδιώτες να αξιοποιήσουν στο έπακρο τα πλεονεκτήματα της τεχνολογίας, αφετέρου, θα περιορίσει τα εμπόδια υιοθέτησής της και θα παράσχει ένα πλαίσιο εμπιστοσύνης. Η κατάλληλη ισορροπία δεν αποτελεί μόνο θεμιτό στόχο, αλλά απαραίτητη προϋπόθεση για το ευοίωνο μέλλον μιας τεχνολογίας, που απαιτεί μια ριζική αναθεώρηση του τρόπου που γίνονται τα πράγματα.

Βιβλιογραφία

Βιβλία

Chohan, U. W., 2017. *The Decentralized Autonomous Organization and Governance Issues,* New South Wales: University of New South Wales (UNSW).

Drescher, D., 2017. *Blockchain Basics. A non technical introduction in 25 steps.* Frankfurt am Main: Apress.

Martinovic, I., 2018. *Blockchains: Design Principles, Applications, and Case Studies.* Oxford: University of Oxford.

Narayanan, A. et al., 2016. *Bitcoin and cryptocurrency technologies: a comprehensive introduction.*. Princeton: Princeton University Press.

ΕΣΔΔΑ, 2018. *Ασφάλεια Ψηφιακών Συστημάτων και Προστασία της Ιδιωτικότητας,* Αθήνα: ΕΚΔΔΑ.

ΕΣΔΔΑ, 2018. *Ανάπτυξη Ανθρώπινου Δυναμικού στην Δημόσια Διοίκηση.* Αθήνα: ΕΚΔΔΑ.

Ζάχος, Ε., Παγουρτζής, Α. & Γροντάς, Π., 2015. *Υπολογιστική Κρυπτογραφία.* Ζωγράφου: ΣΕΑΒ.

Άρθρα – Συμβολές σε Συλλογικούς Τόμους – Εργασίες

Diffie, W. & Hellman, M., 1976. New directions in cryptography. *IEEE Transactions on Information Theory,* 22(6), pp. 644-654.

Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.* s.l.:s.n.

Piscini, E., Guastella, J., Rozman, A. and Nassim, T. (2016). Blockchain: Democratized trust. Distributed ledgers and the future of value. Deloitte University Press.

Κύπρος, Σ., 2018. *Δημιουργία Εφαρμογής Blockchain Ethereum και Κρυπτονομίσματος.* Πειραιάς: Πανεπιστήμιο Πειραιώς.

Νομοθεσία / Νομολογία

Court of Justice of the EU, 2014. *C-461/12 - Granton Advertising,* Court of Justice of the EU.

Ανακοίνωση της Επιτροπής, της 6ης Μαΐου 2015, με τίτλο «Στρατηγική για την ψηφιακή ενιαία αγορά της Ευρώπης» (COM(2015)0192).

Γενική Γραμματεία Ψηφιακής Πολιτικής, 2016. *Εθνική Ψηφιακή Στρατηγική 2016-2021,* Αθήνα: Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης.

Οδηγία 2009/110/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Σεπτεμβρίου 2009, για την ανάληψη, άσκηση και προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος.

ΦΕΚ 28/Α/3-3-1994. *Σύσταση ανεξάρτητης αρχής για την επιλογή προσωπικού και ρύθμιση θεμάτων διοίκησης*.

ΦΕΚ 237/Α/31.10.2014. *Ανοικτή διάθεση και περαιτέρω χρήση εγγράφων, πληροφοριών και δεδομένων του δημόσιου τομέα.*

ΦΕΚ Α' 107/5-5-2014). Πρόσβαση στη δραστηριότητα των πιστωτικών ιδρυμάτων και προληπτική εποπτεία πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων, κατάργηση του ν. 3601/2007 και άλλες διατάξεις.

Εκθέσεις – Αναφορές

DHL Trend Research, 2018. *Perspectives on the upcoming impact of blockchain,* Troisdorf: DHL Customer Solutions & Innovation.

European Cental Bank, 2012. *Virtual Currency Schemes,* Frankfurt am Main: European Cental Bank.

European Central Bank, 2015. *Virtual Currency Schemes, a further analysis,* Frankfurt am Main: European Central Bank.

Gartner, 2018. *2018 Gartner CIO Agenda Survey ,* London.: Gartner.

Furlonger, D. & Kandaswamy, . R., 2018. *Hype Cycle for Blockchain Technologies,* London: Gartner

Global Data, 2018. *Blockchain - Thematic Research,* London: Global Data.

Grech, A. & Camilleri, A. F., 2017. *JRC Science for Policy Report, Blockchain in Education,* Seville: European Commission.

Infosys, 2017. *Breaking barriers: Factors impacting,* Bengaluru: Infosys.

Lantmäteriet, 2016. *The Land Registry In The Blockchain,* s.l.: Lantmäteriet.

World Economic Forum, 2015. *Deep Shift - Technology Tipping Points and Societal Impact.* Geneva: World Economic Forum.

Διαδικτυακές Πηγές

Bheemaiah, K., 2015. *Block Chain 2.0: The Renaissance of Money.* [Online]
Available at: https://www.wired.com/insights/2015/01/block-chain-2-0/
[Accessed 5 November 2018].

Blockchain Hub, 2016. *Blockchains & Distributed Ledger Technologies.* [Online]
Available at: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/
[Accessed 17 November 2018].

Blockchain Support, 2018. *Public and private keys.* [Online]
Available at: https://support.blockchain.com/hc/en-us/articles/360000951966-Public-and-private-keys
[Accessed 16 Novemner 2018].

Buntinx, J., 2017. *What is the Ethereum Virtual Machine.* [Online]
Available at: https://nulltx.com/what-is-the-ethereum-virtual-machine/
[Accessed 18 November 2018].

Buterin, V., 2015. *A Next-Generation Smart Contract and Decentralized Application Platform.* [Online]
Available at: https://github.com/ethereum/wiki/wiki/White-Paper
[Accessed 17 November 2018].

Buterin, V., 2015. *On Public and Private Blockchains.* [Online]
Available at: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
[Accessed 18 November 2018].

Consensys, 2018. *Blockchain Basics.* [Online]
Available at: https://consensys.gitbooks.io/blockchain-in-business/content/subchapter/principles-of-decentralization.html
[Accessed 18 November 2018].

Deloitte, 2017. *Will blockchain transform the public sector?.* [Online]
Available at: https://www2.deloitte.com/insights/us/en/industry/public-sector/understanding-basics-of-blockchain-in-government.html
[Accessed 18 November 2018].

Economist, 2015. *The Trust Machine* [Online]
Available at: https://www.economist.com/leaders/2015/10/31/the-trust-machine
[Accessed 8 November 2018].

European Commission, 2018. *Blockchain Enabled Healthcare.* [Online]
Available at:
http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/imi2-2018-15-02.html
[Accessed 15 November 2018].

European Comimssion, 2018. *European Union Blockchain Observatory and Forum.* [Online]
Available at: https://www.eublockchainforum.eu/about
[Accessed 5 November 2018].

European Commission, 2018. *Blockchain and distributed ledger technologies for SMEs.* [Online]
Available at:
http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/innosup-03-2018.html
[Accessed 15 November 2018].

European Commission, 2018. *Horizon 2020 sections.* [Online]
Available at: https://ec.europa.eu/programmes/horizon2020/h2020-sections
[Accessed 5 December 2018].

European Commission, 2018. *EIC Horizon Prize for 'Blockchains for Social Good'.* [Online]
Available at:
http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/blockchain-eicprize-2019.html
[Accessed 15 November 2018].

European Commission, CORDIS, 2018. *QualiChain.* [Online]
Available at: https://cordis.europa.eu/project/rcn/218758_en.html
[Accessed 8 December 2018].

European Commission, 2018. *European countries join Blockchain Partnership.* [Online]
Available at: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership
[Accessed 16 November 2018].

European Parliament, 2018. *European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation.* [Online]
Available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0373&language=EN&ring=B8-2018-0397
[Accessed 17 November 2018].

Gray, M. & Hajduk, C., 2017. *Anatomy of a Smart Contract.* [Online]
Available at: https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/AnatomyofASmartContract.md
[Accessed 17 November 2018].

Guardtime, 2018. *Cloud Assurance with Blockchains.* [Online]
Available at: https://guardtime.com/solutions/cloud
[Accessed 20 November 2018].

Hooper, M., 2018. *Top five blockchain benefits transforming your industry.* [Online]
Available at: https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/
[Accessed 18 November 2018].

Houlding, D., 2017. *Healthcare Use Cases for Blockchain - 5 Key Factors for Success.* [Online]
Available at: https://www.linkedin.com/pulse/healthcare-use-cases-blockchain-5-key-factors-

houlding-cissp-cipp/
[Accessed 20 November 2018].

Humbeeck, A. V., 2017. *The Blockchain-GDPR Paradox.* [Online]
Available at: https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047
[Accessed 18 November 2018].

Insider, B., 2015. *Goldman Sachs: 'The Blockchain can change...well everything.* [Online]
Available at: http://uk.businessinsider.com/goldman-sachs-the-blockchain-can-change-well-everything-2015-12
[Accessed 6 November 2018].
Investopedia, 2018. *51% Attack.* [Online]
Available at: https://www.investopedia.com/terms/1/51-attack.asp
[Accessed 20 November 2018].

Jayachandran, P., 2017. *The difference between public and private blockchain.* [Online]
Available at: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/
[Accessed 16 November 2018].

Kastelein, R., 2018. *EU Holds Off on Crypto Regulation.* [Online]
Available at: https://www.the-blockchain.com/2018/09/11/eu-holds-off-on-crypto-regulation/
[Accessed 16 November 2018].

Levine, B., 2018. *A new report bursts the blockchain bubble.* [Online]
Available at: https://martechtoday.com/a-new-report-bursts-the-blockchain-bubble-216959
[Accessed 18 November 2018].

Lisk Academy, 2018. *Nodes.* [Online]
Available at: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/nodes
[Accessed 7 November 2018].

Nicholson, S., 2018. *EU Opens Blockchain Observatory, Looking to Invest up to €340 Million.* [Online]
Available at: https://interestingengineering.com/eu-opens-blockchain-observatory-looking-to-invest-up-to-340-million
[Accessed 17 November 2018].

Paul, M. S., 2017. *Hyperledger - When to use the Blockchain Technology.* [Online]
Available at: https://medium.com/swlh/hyperledger-chapter-3-when-to-use-the-blockchain-technology-a5c414221bdf
[Accessed 20 November 2018].

Rabbani, H., 2017. *What is Hashing & Digital Signature in The Blockchain.* [Online]
Available at: https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/
[Accessed 7 Novemner 2018].

Rizzo, P., 2016. *How Barclays Used R3's Tech to Build a Smart Contracts Prototype.* [Online]
Available at: http://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda/
[Accessed 6 November 2018].

Sardan, T., 2018. *What is a light client and why you should care.* [Online]
Available at: https://www.parity.io/what-is-a-light-client/
[Accessed 15 November 2018].

Strukhoff, R., 2016. *When Is a Private Blockchain a Good Idea, and When Is It Not.* [Online]
Available at: https://www.altoros.com/blog/when-is-a-private-blockchain-a-good-idea-and-when-is-it-not/
[Accessed 17 November 2018].

Swan, M., 2018. *Blockchain 1.0: Currency*. [Online]
Available at: https://www.oreilly.com/library/view/blockchain/9781491920480/ch01.html
[Accessed 16 November 2018].

Thompson, C., 2016. *How does the Blockchain Work?*. [Online]
Available at: https://medium.com/blockchain-review/blockchain-essentials-for-dummies-ba2d8851f1ca
[Accessed 8 November 2018].

Trujillo, J. L., Fromhart, S. & Srinivas, V., 2017. *Evolution of blockchain technology. Insights from the GitHub platform.* [Online]
Available at: https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html
[Accessed 20 November 2018].

Tuwiner, J., 2018. *Bitcoin Mining Pools.* [Online]
Available at: https://www.buybitcoinworldwide.com/mining/pools/
[Accessed 20 November 2018].

Unibright, 2017. *Blockchain evolution: from 1.0 to 4.0.* [Online]
Available at: https://medium.com/@UnibrightIO/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666
[Accessed 17 November 2018].

White, M. & Killmeyer, J., 2017. *Will blockchain transform the public sector?.* [Online]
Available at: https://www2.deloitte.com/insights/us/en/industry/public-sector/understanding-basics-of-blockchain-in-government.html
[Accessed 25 November 2018].

Williams, A., 2016. *IBM to open first blockchain innovation centre in Singapore.* [Online]
Available at: https://www.straitstimes.com/business/economy/ibm-to-open-first-blockchain-innovation-centre-in-singapore-to-create-applications
[Accessed 5 November 2018].

Γενική Γραμματεία Ψηφιακής Πολιτικής, 2018. *Συμμετοχή του Γ.Γ. Ψηφιακής Πολιτικής στο 2ο Μαραθώνιο Καινοτομίας.* [Online]
Διαθέσιμο στο: http://mindigital.gr/index.php/41-ggpsp/media/2438-symmetoxi-tou-g-g-ps-p-sto-crowdhachathon-tis-kede
[Πρόσβαση: 8 Δεκέμβριος 2018].

Υπουργείο Ψηφιακής Πολιτικής, 2018. *Υπογραφή της Διυπουργικής Διακήρυξης χωρών της Ν. Ευρώπης για τις Τεχνολογίες Κατανεμημένου Καθολικού (blockchain).* [Online]
Διαθέσιμο στο: http://mindigital.gr/index.php/41-ggpsp/media/3259-blockchain-4-2018
[Πρόσβαση: 5 Δεκέμβριος 2018].

Λογαράς, Κ., 2018. *Η Τεχνολογία Blockchain, οι εφαρμογές και οι νομικές πτυχές της.* [Online]
Διαθέσιμο στο: https://www.lawspot.gr/nomika-nea/h-tehnologia-blockchain-oi-efarmoges-kai-oi-nomikes-ptyhes-tis#footnoteref8_o3i808b
[Πρόσβαση: 15 Νοέμβριος 2018].

Εθνική Σχολή Δημόσιας Διοίκησης και Αυτοδιοίκησης (ΕΣΔΔΑ)
Πειραιώς 211, ΤΚ 177 78, Ταύρος
τηλ: 2131306349 , fax: 2131306479
www.ekdd.gr