Η ΕΞΕΛΙΞΗ ΤΩΝ BLOCKCHAIN ΜΕΤΑ ΤΟ BITCOIN

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΚΑΤΕΥΘΥΝΣΗ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΣ ΚΑΙ ΕΤΑΙΡΕΙΩΝ ΝΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΓΙΑ ΣΤΕΛΕΧΗ

ΛΑΜΠΡΙΝΤΖΗΣ ΠΑΝΑΓΙΩΤΗΣ (Α.Μ. 1526)

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΓΙΑΓΛΗΣ ΓΕΩΡΓΙΟΣ

Αθήνα, Νοέμβριος 2017

Αθήνα, Νοέμβριος 2017

ΕΥΧΑΡΙΣΤΙΕΣ

Ευχαριστώ θερμά τον καθηγητή του Ο.Π.Α. κύριο Γιαγλή Γεώργιο για την συμβολή του στην εκπόνηση της παρούσας εργασίας.

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

«Δηλώνω υπεύθυνα ότι η συγκεκριμένη μεταπτυχιακή διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών του Διατμηματικού ΠΜΣ των Τμημάτων Οργάνωσης και Διοίκησης Επιχειρήσεων και Μάρκετινγκ και Επικοινωνίας του Οικονομικού Πανεπιστημίου Αθηνών στη Διοίκηση Επιχειρήσεων: MBA (Master in Business Administration) με κατεύθυνση στην Οργάνωση και Διοίκηση Τηλεπικοινωνιακών Επιχειρήσεων και Εταιρειών Νέας Τεχνολογίας για στελέχη έχει συγγραφεί από εμένα προσωπικά και δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό. Η εργασία αυτή έχοντας εκπονηθεί από εμένα, αντιπροσωπεύει τις προσωπικές μου απόψεις επί του θέματος. Οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης διπλωματικής αναφέρονται στο σύνολό τους, δίνοντας πλήρεις αναφορές στους συγγραφείς, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο».

ΕΙΣΑΓΩΓΗ

Η παρούσα εργασία στοχεύει στο να παρουσιάσει την εξέλιξη των Blockchain μετά το Bitcoin. Σκοπός είναι η εισαγωγή του αναγνώστη στο χώρο της νέας τεχνολογίας.

Αρχικά, εξετάζονται οι έννοιες γύρω από την τεχνολογία Blockchain μέσω του παραδείγματος του Bitcoin - που ουσιαστικά υπήρξε το πρώτο δίκτυο Blockchain. Ο παραλληλισμός γίνεται διότι την χρονική στιγμή της συγγραφής της παρούσας εργασίας, το ευρύ κοινό είναι εξοικειωμένο κυρίως με το Bitcoin και θεωρούμε πως με τον τρόπο αυτό, οι σχετικές με την νέα τεχνολογία έννοιες θα είναι περισσότερο ευκολονόητες από τον αναγνώστη.

Στη συνέχεια, εξετάζεται το οικοσύστημα του Ethereum και οι έννοιες που εισήγαγε στον χώρο των Blockchains, όπως τα Έξυπνα Συμβόλαια (Smart Contracts), τα Decentralized Apps [dApps], τα Initial Coin Offerings [ICOs] και τα Distributed Autonomous Organizations [DAOs].

Στο σημείο αυτό της εργασίας, ο αναγνώστης έχει πληροφορηθεί για τα δημόσια (public) Blockchains και τα σχετικά κρυπτονομίσματα. Επίσης, ο αναγνώστης μπορεί να διακρίνει μεταξύ της πρώτης γενιάς Blockchain που υπήρξε το Bitcoin - όπου ουσιαστικά το Blockchain του Bitcoin δημιουργήθηκε αποκλειστικά για να εξυπηρετεί το κρυπτονόμισμα bitcoin [BTC] – και της δεύτερης γενιάς που υπήρξε το Ethereum – όπου πλέον το κρυπτονόμισμα Ether [ETH] εξυπηρετεί το Blockchain του Ethereum και όχι το αντίστροφο.

Στα επόμενα κεφάλαια παρουσιάζεται η τρίτη γενιά Blockchains, δηλαδή τα private Permissioned Blockchains (ή Distributed Ledger Technologies [DLTs], όπως συχνά αποκαλούνται) και συγκεκριμένα τα οικοσυστήματα των Hyperledger και R3 Corda.

Ακολούθως, πραγματοποιείται σύγκριση μεταξύ του public Permissionless Blockchain του Ethereum και των private Permissioned μοντέλων που χαρακτηρίζουν τη λειτουργία των Hyperledger Fabric και R3 Corda. Στο σημείο αυτό, ο αναγνώστης είναι σε θέση να διακρίνει τις βασικές διαφορές - τόσο σε επίπεδο τεχνολογίας όσο και ως προς τις εφαρμογές κάθε λύσης – μεταξύ των public Permissionless Blockchains και των private Permissioned DLTs.

Στη συνέχεια, εξετάζεται η συσχέτιση της εξέλιξης των Blockchains με την υιοθέτηση της νέας τεχνολογίας από τον τραπεζικό τομέα και παρουσιάζονται σχετικές εφαρμογές, ενώ στο τελευταίο κεφάλαιο παρατίθενται εφαρμογές της τεχνολογίας Blockchain σε διάφορους κλάδους, όπως έχουν δημοσιευτεί στον διεθνή τύπο.

Λέξεις Κλειδιά

Blockchain, Smart Contracts, Decentralized Applications, Initial Coin Offerings, Distributed Autonomous Organization, Consensus, Distributed Ledger Technologies

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 7: ΕΦΑΡΜΟΓΕΣ ΤΩΝ BLOCKCHAINS

ΕΙΚΟΝΕΣ

ΚΕΦΑΛΑΙΟ 1: BLOCKCHAIN ΚΑΙ BITCOIN

1.1Τι είναι το Blockchain

Μια αλυσίδα από μπλοκ - ή αλλιώς ένα Blochchain - είναι ουσιαστικά μια κατανεμημένη βάση δεδομένων, που ως εγγραφές περιέχει αρχείο όλων των συναλλαγών ή ψηφιακών γεγονότων που έχουν εκτελεστεί και μοιραστεί μεταξύ των συμβαλλόμενων μερών, εντός του δικτύου που σχηματίζουν όλοι οι κόμβοι που συμμετέχουν στην πλατφόρμα του Blockchain. (Berkeley's Applied Innovation Review, Issue No.2, June 2016).

Το Blockchain δηλαδή, είναι ένα δημόσιο καθολικό καταγραφής συναλλαγών, με τη μορφή μιας συνεχώς αναπτυσσόμενης λίστας εγγραφών, που ονομάζονται blocks, οι οποίες συσχετίζονται και διαφυλάσσονται μέσω κρυπτογραφίας. Λόγω του σχεδιασμού τους, τα blockchains έχουν έμφυτους μηχανισμούς προστασίας ενάντια στην αλλοίωση των δεδομένων. Όλοι οι κόμβοι, που χαρακτηρίζονται από την έλλειψη κεντρικού ελέγχου, διατηρούν συγχρόνως και με αυτό τον τρόπο επικυρώνουν τις πληροφορίες που περιέχονται στα μπλοκ, ενώ το πρωτόκολλο κοινής συναίνεσης (consensus protocol) διασφαλίζει τη συμφωνία των κόμβων ως προς την μοναδική δομή των εγγραφών.

1.2Ανάλυση του Blockchain

Ένα μπλοκ αποτελεί ένα αυτούσιο κομμάτι της αλυσίδας, στο οποίο καταγράφονται όλες οι τελευταίες χρονικά συναλλαγές που πραγματοποιούνται στο δίκτυο των κόμβων που συμμετέχουν στην πλατφόρμα. Όταν ολοκληρωθεί ένα μπλοκ τότε εισάγεται στην αλυσίδα ως μια μόνιμη βάση δεδομένων. Ένα νέο μπλοκ

δημιουργείται κάθε φορά που το προηγούμενο μπλοκ ολοκληρώνεται. Τα πολυάριθμα μπλοκ που σχηματίζουν την αλυσίδα των μπλοκ συνδέονται μεταξύ τους (όπως οι κρίκοι μιας αλυσίδας) γραμμικά και σε χρονολογική σειρά. Κάθε μπλοκ περιέχει αναφορά στο προηγούμενο μπλοκ. Η αλυσίδα των μπλοκ συνολικά περιέχει κάθε πληροφορία που αφορά όλες τις διευθύνσεις χρηστών και το υπόλοιπο σε αξία καθεμίας από αυτές, ξεκινώντας από το αρχικό μπλοκ και φτάνοντας μέχρι και το τελευταίο χρονικά ολοκληρωμένο μπλοκ.

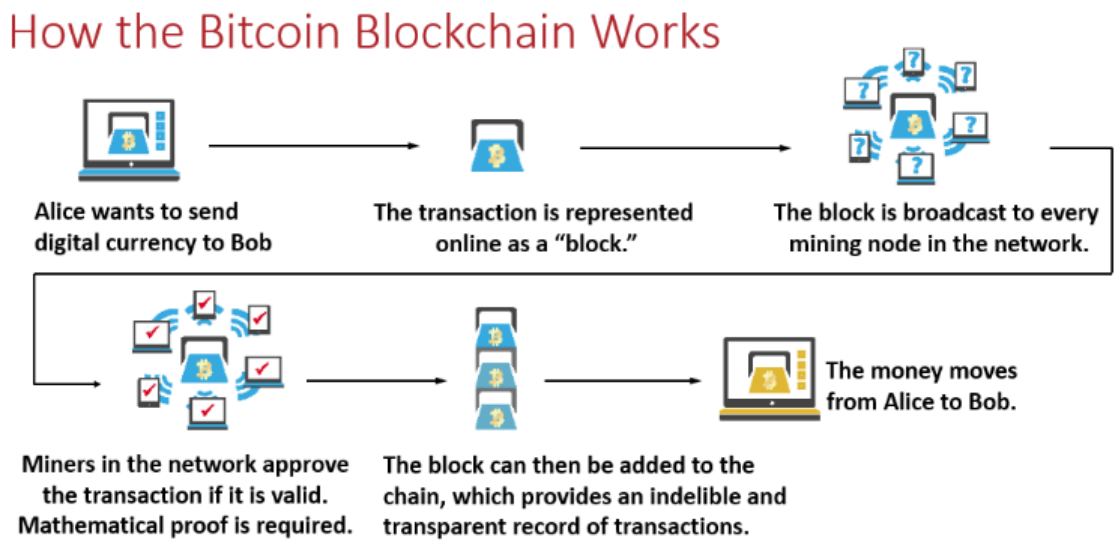
Η τεχνολογία της αλυσίδας των μπλοκ έχει σχεδιαστεί ώστε τα δεδομένα που περιέχονται να είναι αμετάβλητα, δηλαδή να μην είναι δυνατή η διαγραφή τους. Μετά την καταγραφή των δεδομένων σε κάποιο μπλοκ, αυτά μεταγενέστερα είναι αδύνατο να τροποποιηθούν, αφού κάτι τέτοιο θα απαιτούσε επίσης την τροποποίηση όλων των επόμενων χρονικά μπλοκ της αλυσίδας – γεγονός που θα απαιτούσε με τη σειρά του την κοινή συναίνεση όλων των κόμβων του δικτύου για να πραγματοποιηθεί.

1.3 Blockchain και Bitcoin

Η τεχνολογία της αλυσίδας των μπλοκ αναπτύχθηκε αρχικά ως η λογιστική μέθοδος για το ψηφιακό νόμισμα Bitcoin και ίσως αποτελεί την σημαντικότερη καινοτομία που εισήγαγε η νέα τεχνολογία. Η λειτουργία του Bitcoin δεν ρυθμίζεται από κάποια κεντρική αρχή. Αντίθετα, οι χρήστες του πραγματοποιούν και επιβεβαιώνουν συναλλαγές κάθε φορά που κάποιος πληρώνει σε κάποιον άλλο (ή κάποιους άλλους) το αντίτιμο για την πώληση αγαθών ή υπηρεσιών, εξαλείφοντας με αυτόν τον τρόπο την ανάγκη κάποια τρίτη οντότητα να διεκπεραιώνει τις πληρωμές και να κρατάει πλήρες αρχείο όλων των δεδομένων που αφορούν τις συναλλαγές. Η ολοκληρωμένη συναλλαγή καταγράφεται στο δημόσιο κατανεμημένο καθολικό, ως εγγραφή σε

μπλοκ και τελικά στην αλυσίδα των μπλοκ, όπου επιβεβαιώνεται από το σύνολο των κόμβων του δικτύου. Κατά μέσο όρο, ένα νέο μπλοκ προστίθεται στην αλυσίδα των μπλοκ, μέσω της διαδικασίας εξόρυξης (mining), η οποία θα αναλυθεί στη συνέχεια.

Ακολούθως παρατίθεται διαγράμματα της διαδικασίας συναλλαγής μεταξύ χρηστών στο Bitcoin, από σχετικό άρθρο του Coug Sleeter στην ιστοσελίδα Accountex Report:



Εικόνα 1: How the Bitcoin Blockchain Works (Doug Sleeter,2017)

Βάσει του πρωτοκόλλου του Bitcoin, το σύνολο των δεδομένων της αλυσίδας των μπλοκ διαμοιράζεται μεταξύ του συνόλου των κόμβων που συμμετέχουν στο σύστημα. Κατά την σύνδεση ενός χρήστη στο δίκτυο του Blockchain, ο υπολογιστής που συνδέεται στο δίκτυο κατεβάζει αυτόματα ένα αντίγραφο ολόκληρης της αλυσίδας των μπλοκ, η οποία περιέχει αρχείο όλων των συναλλαγών που έχουν ποτέ εκτελεστεί στο Bitcoin – εξυπηρετώντας με αυτόν τον τρόπο την ανάγκη επιβεβαίωσης της ορθότητας των περιεχόμενων στα μπλοκ δεδομένων και άρα των ίδιων των συναλλαγών. Συνεπώς, η αλυσίδα των μπλοκ περιέχει δεδομένα για όλα τα ποσά (αξίες) που ανήκαν σε κάθε διεύθυνση, για οποιοδήποτε χρονικό σημείο του παρελθόντος.

1.3.1 Mining και Bitcoin

Στην παρούσα ενότητα και για λόγους συνέχειας των εννοιών στα πλαίσια της εργασίας, θα αναφερθούμε στη διαδικασία εξόρυξης στο Bitcoin.

Στο Bitcoin, η διαδικασία της εξόρυξης εξυπηρετεί δύο ιδιαίτερα σημαντικούς σκοπούς. Αφενός, μέσω της εξόρυξης παράγονται νέες μονάδες Bitcoin, όπως θα αναλυθεί στη συνέχεια. Παράλληλα όμως, μέσω της διαδικασίας αυτής, τα δεδομένα που αφορούν τις συναλλαγές εισάγονται στα μπλοκ και τελικά στην αλυσίδα των μπλοκ, επιβεβαιώνοντας με αυτόν τον τρόπο την γνησιότητα των συναλλαγών και συμβάλλοντας στην ασφάλεια του δικτύου του Bitcoin. Η διαδικασία της εξόρυξης περιλαμβάνει τη σύνθεση όλων των δεδομένων που αφορούν τις πρόσφατες συναλλαγές σε μπλοκ, ενώ παράλληλα όλοι οι κόμβοι που συμμετέχουν καταναλώνουν επεξεργαστική ισχύ με σκοπό την επίλυση ενός σύνθετου υπολογιστικού προβλήματος. Ο πρώτος συμμετέχον που επιλύει το πρόβλημα είναι ο κόμβος που τοποθετεί το νέο μπλοκ στην αλυσίδα των μπλοκ και λαμβάνει τις σχετικές ανταμοιβές. Οι ανταμοιβές αυτές αποτελούν τα κίνητρα για τους χρήστες που συμμετέχουν στην διαδικασία εξόρυξης και περιλαμβάνουν τόσο την ανταμοιβή για την καταγραφή των συναλλαγών στην αλυσίδα των μπλοκ, όσο και τα νεοδημιουργηθέντα νομίσματα BTC. Μία διαγραμματική απεικόνιση της παραπάνω περιγραφής παρουσιάζεται στην εικόνα που ακολουθεί:

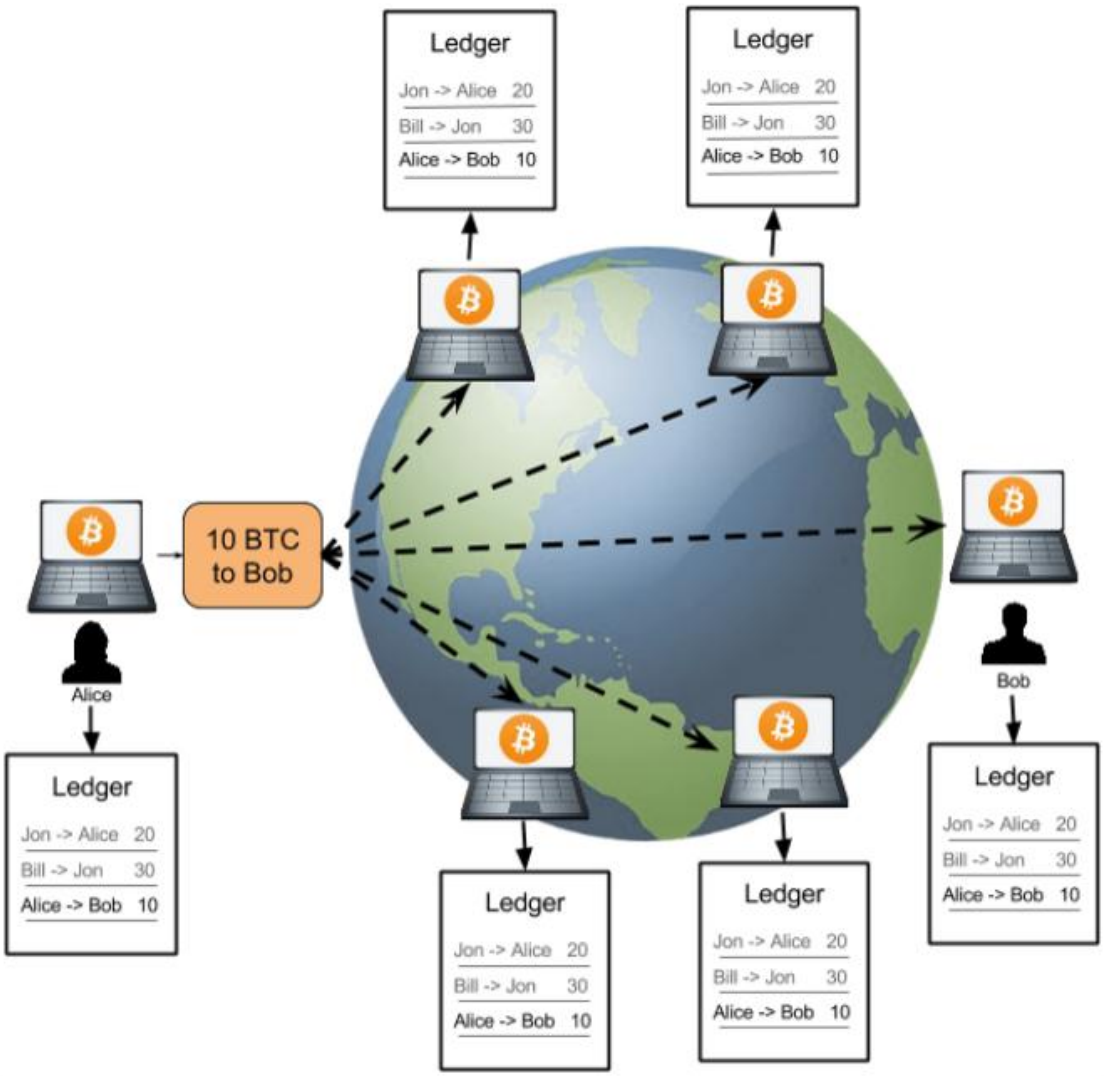


Figure 2 – The global network of Bitcoin mining nodes.

Εικόνα 2: The global network of Bitcoin mining nodes (Doug Sleeter,2017)

1.3.2 Mining και ασφάλεια του δικτύου Bitcoin

Η εξόρυξη (mining) είναι μια αποκεντρωμένη διαδικασία. Κάθε χρήστης με πρόσβαση σε σύνδεση διαδικτύου και το κατάλληλο υλισμικό μπορεί να συμμετέχει σε αυτή. Η ασφάλεια του δικτύου του Bitcoin εξαρτάται από τον αποκεντρωμένο του χαρακτήρα, αφού το δίκτυο παίρνει αποφάσεις βάσει κοινής συναίνεσης (consensus) . Σε περίπτωση διαφωνίας σχετικά με την ορθότητα των δεδομένων ενός μπλοκ – και άρα σχετικά με το αν θα πρέπει το μπλοκ αυτό να προστεθεί στην αλυσίδα των μπλοκ

– το σύστημα οδηγείται σε απόφαση ουσιαστικά μέσω της συμφωνίας (ή κοινής συναίνεσης) της πλειοψηφίας των κόμβων του δικτύου και συγκεκριμένα όταν περισσότερη από την μισή επεξεργαστική ισχύ του δικτύου συμφωνεί.

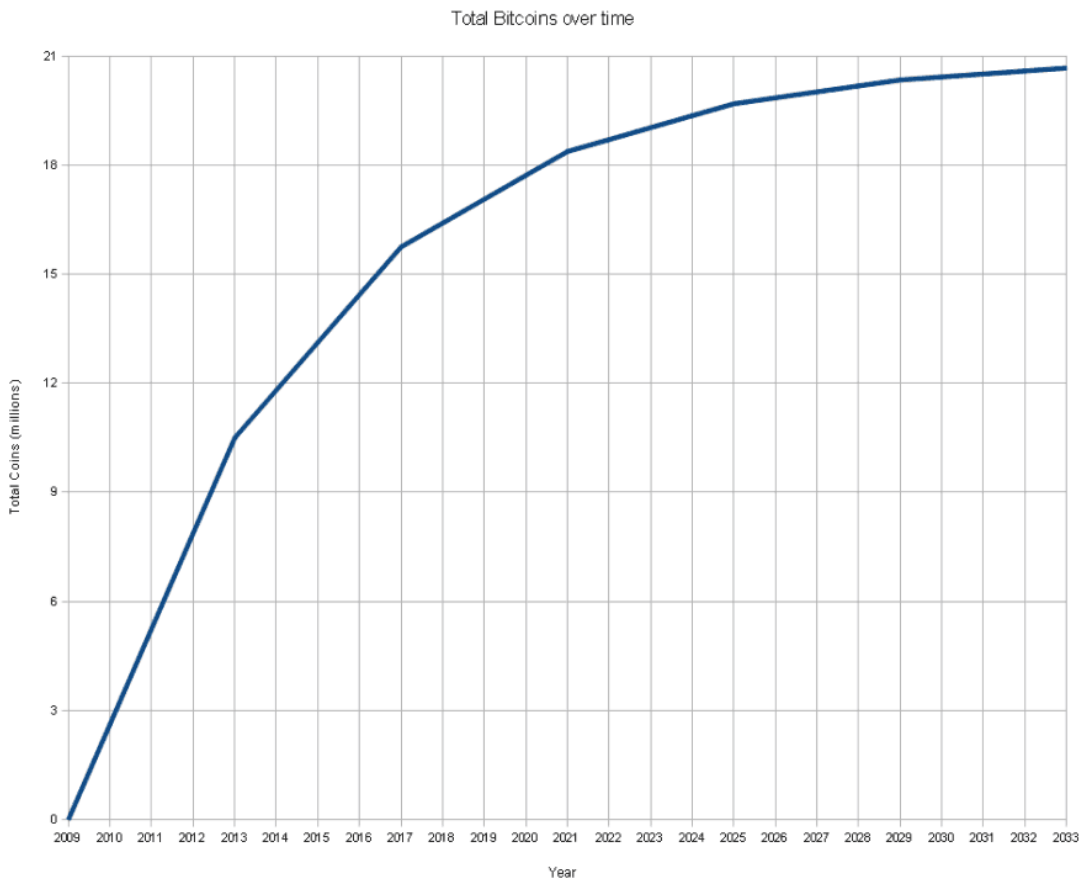
Συνεπώς, εάν θεωρητικά ένα χρήστης ή ένας οργανισμός ελέγχει περισσότερη από την μισή επεξεργαστική ισχύ του δικτύου του Bitcoin, τότε έχει τη δύναμη να αλλοιώσει τα δεδομένα της αλυσίδας των μπλοκ. Η έννοια του ελέγχου της περισσότερης από τη μισή συνολικά επεξεργαστική ισχύ του δικτύου με σκοπό την αλλοίωση της αλυσίδας των μπλοκ είναι γνωστή ως «επίθεση του 51%» ή "51% attack". Με βάση τα παραπάνω, το πόσο κοστοβόρα θα ήταν μια τέτοια επίθεση στο δίκτυο εξαρτάται άμεσα από την επεξεργαστική ισχύ που αναλώνεται συνολικά στο δίκτυο του Bitcoin. Συνεπώς, η ασφάλεια του εν λόγω δικτύου είναι άμεση συνάρτηση της επεξεργαστικής ισχύος που απαιτείται συνολικά για τη διαδικασία εξόρυξης. Τέλος, αξίζει να σημειωθεί πως το ποσό της επεξεργαστικής ισχύος που αναλώνεται στο δίκτυο εξαρτάται από το πόσο ελκυστικά είναι τα κίνητρα που ελκύουν τους χρήστες στη διαδικασίας της εξόρυξης, τα οποία αποτελούνται από την ανταμοιβή μπλοκ (block reward) και τις ανταμοιβές για την καταγραφή των συναλλαγών σε μπλοκ.

Στο σημείο αυτό αξίζει να γίνει ιδιαίτερη αναφορά στο γεγονός ότι η επιβεβαίωση των συναλλαγών μέσω της εγγραφής όλων των δεδομένων που τις αφορούν, χωρίς εξαίρεση, στο διαμοιρασμένο δημόσιο καθολικό προστατεύει το σύστημα από φαινόμενα απάτης Διπλής Δαπάνης (Double Spending problem) (Investopedia). Το πρόβλημα της Διπλής Δαπάνης αφορά την περίπτωση που η ίδια μονάδα ψηφιακού νομίσματος μπορεί να ξοδευτεί δύο φορές. Είναι ένα πρόβλημα που αφορά ιδιαίτερα τα ψηφιακά νομίσματα, αφού η ψηφιακή πληροφορία μπορεί να αναπαραχθεί σχετικά εύκολα σε σύγκριση με τα φυσικά συναλλάγματα. Ο κάτοχος κάποιου ψηφιακού

νομίσματος μπορεί θεωρητικά να δημιουργήσει ένα αντίγραφο της νομισματικής μονάδας και στη συνέχεια να το αποστείλει σε κάποιον τρίτο, διατηρώντας παράλληλα το πρωτότυπο. Η ανησυχία γύρω από το θέμα αυτό εμφανίστηκε αρχικά σχετικά με το Bitcoin, αφού είναι ένα αποκεντρικοποιημένο νόμισμα, χωρίς κάποια κεντρική αρχή ελέγχου ικανή να διασφαλίζει πως κάθε νόμισμα ξοδεύεται μόνο μία φορά.

1.3.3 Block Reward στο Bitcoin

Επανερχόμενοι στο ζήτημα της δημιουργίας νέων μονάδων Bitcoin μέσω της εξόρυξης, ακολούθως αναλύουμε σημαντικούς όρους και παραθέτουμε ποσοτικά στοιχεία για την όλη διαδικασία. Το πλήθος των μονάδων Bitcoin που ελευθερώνονται με κάθε εξόρυξη ενός μπλοκ ονομάζεται ανταμοιβή μπλοκ (block reward). Το πλήθος των κρυπτονομισμάτων που αποτελεί μια ανταμοιβή μπλοκ μειώνεται στο μισό μετά τη δημοσίευση 210.000 μπλοκ στην αλυσίδα των μπλοκ ή προσεγγιστικά κάθε τέσσερα έτη. Αρχικά, η ανταμοιβή των μπλοκ το 2009 ξεκίνησε με 50 μονάδες Bitcoin, μειώθηκε στο μισό το 2012, δηλαδή στις 25 μονάδες και ξανά το 2016 μειώθηκε στις 12.5 μονάδες. Η πτωτική αυτή πορεία του πλήθους των κρυπτονομισμάτων που αποτελούν την ανταμοιβή για την εξόρυξη ενός μπλοκ, οδηγεί με βεβαιότητα σε ένα πεπερασμένο πλήθος μονάδων Bitcoin που είναι δυνατόν να παραχθούν συνολικά. Συγκεκριμένα, το σύνολο των μονάδων Bitcoin που μπορούν να παραχθούν υπολογίζεται στις 21.000.000 μονάδες και η διαδικασία αναμένεται να ολοκληρωθεί το 2140, οπότε και αναμένεται να παραχθεί η τελευταία μονάδα BTC.



Εικόνα 3: Total Bitcoins over time (Wikipedia)

1.3.4 Transaction fees στο Bitcoin

Οι ανταμοιβές για την καταγραφή των συναλλαγών σε μπλοκ αποτελούνται από το ποσό των μονάδων Bitcoin που περιέχεται σε κάθε συναλλαγή, ως αμοιβή για τον χρήστη που εξορύσσει το μπλοκ στο οποίο σώζονται τα δεδομένα που αφορούν την εν λόγω συναλλαγή. Τα τέλη που αφορούν κάθε συναλλαγή πληρώνονται οικειοθελώς από τον χρήστη που εκτελεί την συναλλαγή. Επίσης, το αν μια συναλλαγή θα προστεθεί σε μπλοκ από κάποιον συγκεκριμένο χρήστη προϋποθέτει την οικειοθελή κατανάλωση της απαιτούμενης επεξεργαστικής ισχύος από αυτόν. Συνεπώς, οι χρήστες που επιθυμούν να εκτελέσουν μια συναλλαγή μπορούν να

θεωρήσουν τα τέλη συναλλαγής ως ένα κίνητρο προς άλλους χρήστες, ώστε οι τελευταίοι να επικυρώσουν την εν λόγω συναλλαγή μέσω της εξόρυξης.

ΚΕΦΑΛΑΙΟ 2: ETHEREUM

2.1 Η ιστορία του Ethereum

Το Ethereum περιγράφτηκε αρχικά από τον Vitalik Buterin, περί τα τέλη του 2013 ως αποτέλεσμα της έρευνας και της εμπλοκής του με την κοινότητα του Bitcoin. Στη συνέχεια, ο Vitalik δημοσίευσε τη Λευκή Βίβλο για το Ethereum, όπου περιγράφει με λεπτομέρεια τόσο τον σχεδιασμό σε τεχνικό επίπεδο, όσο και τους σκοπούς που εξυπηρετούν το πρωτόκολλο του Ethereum και η αρχιτεκτονική των Έξυπνων Συμβολαίων (Smart Contracts). Τον Ιανουάριο του 2014, ο Vitalik ανακοίνωσε επίσημα το εγχείρημα Ethereum στο συνέδριο Bitcoin της Βόρειας Αμερικής, στο Μαϊάμι των Ηνωμένων Πολιτειών Αμερικής.

Την ίδια περίοδο, ο Vitalik ξεκίνησε τη συνεργασία του με τον Δρ. Gavin Wood και μαζί ιδρύσανε το Ethereum. Τον Απρίλιο του 2014, ο Gavin δημοσίευσε επιστημονική εργασία για το Ethereum, περιγράφοντας λεπτομερώς τις τεχνικές προδιαγραφές για την ανάπτυξη του Ethereum Virtual Machine (EVM), το οποίο θα αναλυθεί στη συνέχεια και ουσιαστικά αποτελεί το περιβάλλον στο οποίο εκτελούνται οι εφαρμογές Έξυπνων Συμβολαίων στο Ethereum.

2.1.1 Το ίδρυμα Ethereum (Ethereum Foundation) και η προπώληση των μονάδων Ether

Η ανάπτυξη ενός νέου κρυπτονομίσματος και ενός Blockchain απαιτεί πόρους. Η ομάδα του Ethereum, στην προσπάθειά της να κινητοποιήσει ένα μεγάλο δίκτυο από προγραμματιστές, χρήστες για εξόρυξη, επενδυτές και άλλες ομάδες ενδιαφερομένων, ανακοίνωσε τα σχέδιά της για την υλοποίηση ενός σχεδίου προπώλησης μονάδων Ether - της μονάδας συναλλάγματος του Ethereum. Η

πολυπλοκότητα σε νομικό επίπεδο, αυτού του εγχειρήματος συγκέντρωσης κεφαλαίων μέσω της προπώλησης των κρυπτονομισμάτων οδήγησε στη δημιουργία πληθώρας νομικών προσώπων, με κυριότερο το Ίδρυμα Ethereum (Ethereum Foundation), που συστάθηκε τον Ιούνιο του 2014 στην Ελβετία.

Τον Ιούλιο του 2014, η ομάδα του Ethereum πραγματοποίησε την πρώτη διανομή μονάδων Ether μέσω μια δημόσιας διαδικασίας προπώλησης των κρυπτονομισμάτων, που διήρκησε 42 ημέρες. Συγκεντρώθηκαν 31,951 μονάδες bitcoin - που τη συγκεκριμένη χρονική στιγμή είχαν αξία 18,439,085 Δολαρίων Η.Π.Α – με αντάλλαγμα 60,102,216 μονάδες Ether. Τα κέρδη του εγχειρήματος χρησιμοποιήθηκαν για την αποπληρωμή χρεών και για την χρηματοδότηση της ανάπτυξης του Ethereum.

Η ομάδα του Ethereum, μέσω την προπώλησης των μονάδων Ether ουσιαστικά οργάνωσε μια Αρχική Προσφορά Νομισμάτων - Initial Coin Offering, ή όπως συχνότερα αποκαλείται, ένα ICO. Τα ICOs θα αναλυθούν σε επόμενη ενότητα.

2.2 Εισαγωγή στο Ethereum

Το Ethereum είναι λογισμικό το οποίο εκτελείται σε ένα δίκτυο υπολογιστών, όπου τα δεδομένα και τα επιμέρους προγράμματα που ονομάζονται Έξυπνα Συμβόλαια αντιγράφονται και εκτελούνται παράλληλα σε όλους τους υπολογιστές που αποτελούν το σύνολο των κόμβων του δικτύου, χωρίς κάποια κεντρική αρχή να συντονίζει την όλη διαδικασία. Τα επιμέρους προγράμματα ονομάζονται Έξυπνα Συμβόλαια και αυτά εκτελούνται στους υπολογιστές - κόμβους του δικτύου μέσω του Λειτουργικού που ονομάζεται Ethereum Virtual Machine (EVM).

Το Ethereum επεκτείνει τις έννοιες γύρω από την τεχνολογία Blockchain σε σχέση με το Bitcoin, στο οποίο τα δεδομένα που αφορούν τις συναλλαγές αποθηκεύονται σε πολυάριθμους υπολογιστές παγκοσμίως. Με το Ethereum γίνεται ένα επιπλέον βήμα μπροστά σε επίπεδο τεχνολογίας, αφού πέραν της καταγραφής δεδομένων στους κόμβους του δικτύου, πλέον είναι δυνατή και η εκτέλεση υπολογιστικού κώδικα παράλληλα σε πολυάριθμους υπολογιστές, που βρίσκονται σε διαφορετικά σημεία του πλανήτη.

Το όραμα πίσω από το εγχείρημα του Ethereum είναι η δημιουργία ενός παγκόσμιου κατανεμημένου υπέρ-υπολογιστή, αυτοσυντηρούμενου και η λειτουργία του οποίου να μην υπόκειται σε κεντρικό έλεγχο από κάποια αρχή.

Βασικό σημείο καινοτομίας που εισήγαγε το Ethereum στην τεχνολογία των αλυσίδων από μπλοκ αποτελούν τα Έξυπνα Συμβόλαια. Για το λόγο αυτό, την παρούσα ενότητα ακολουθεί η ανάλυση της έννοιας των Έξυπνων Συμβολαίων.

2.3 Εισαγωγή στα Έξυπνα Συμβόλαια

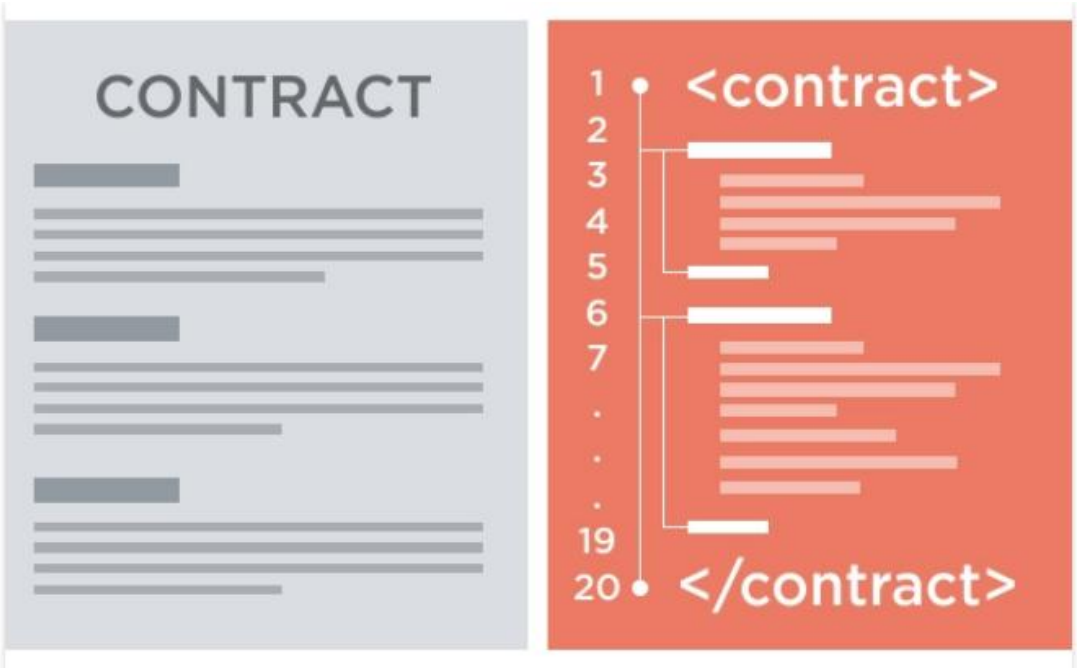
2.3.1 Συμβόλαια

Συμβόλαιο ή σύμβαση είναι κάθε οικειοθελής συμφωνία μεταξύ δύο η περισσότερων μερών, η οποία εφαρμόζεται διά νόμου. Η νομοθεσία περί συμβολαίων αφορά τα δικαιώματα και τις υποχρεώσεις που προκύπτουν στα πλαίσια συμφωνιών και ένα συμβόλαιο προκύπτει όταν δύο ή περισσότερα μέρη καταλήγουν σε συμφωνία. Στην καθημερινή ζωή, οι περισσότερες συμβάσεις μπορεί να είναι προφορικές, όπως μια απλή συναλλαγή πώλησης. Πολλές φορές όμως, γραπτές συμφωνίες απαιτούνται είτε από τα συμβαλλόμενα μέρη, εκ του νόμου ή από το νόμο στο πλαίσιο διαφορών

δικαιοδοσίας για ορισμένα είδη συμφωνιών, για παράδειγμα κατά την αγορά ενός σπιτιού ή γης (Wikipedia).

2.3.2 Έξυπνα Συμβόλαια

Η έννοια του έξυπνου συμβολαίου προτάθηκε για πρώτη φορά από τον Nick Szabo το 1996. Η βασική ιδέα πίσω από τα έξυπνα συμβόλαια είναι πως όροι συμβολαίων διαφόρων ειδών, όπως επισχέσεις, εγγυήσεις, δικαιώματα ιδιοκτησίας κ.α. μπορούν να ενσωματωθούν στο υλισμικό και λογισμικό που η ανθρωπότητα χρησιμοποιεί, με τρόπο ώστε να καθίσταται δύσκολη ή και αδύνατη η αλλοίωση του περιεχόμενου του συμβολαίου. Θα μπορούσε κανείς να πει πως, πρόγονος των Έξυπνων Συμβολαίων υπήρξαν τα μηχανήματα αυτόματης πώλησης. Ο αυτόματος πωλητής είναι ουσιαστικά μια συσκευή που εφαρμόζει αυτόματα κάποιους προσυμφωνημένους κανόνες, δηλαδή το μηχάνημα δέχεται χρήματα και αυτόματα ελευθερώνει τη διαφορά από το αντίτιμο και το προϊόν. Όπως ο αυτόματος πωλητής εφαρμόζοντας ένα ασύγχρονο πρωτόκολλο φέρνει σε επαφή την εταιρεία αναψυκτικών με τον πελάτη, τα έξυπνα συμβόλαια μπορούν να επιβάλουν κάποιους όρους με σύγχρονο τρόπο σε δύο ή περισσότερα συμβαλλόμενα μέρη (Szabo,1996).

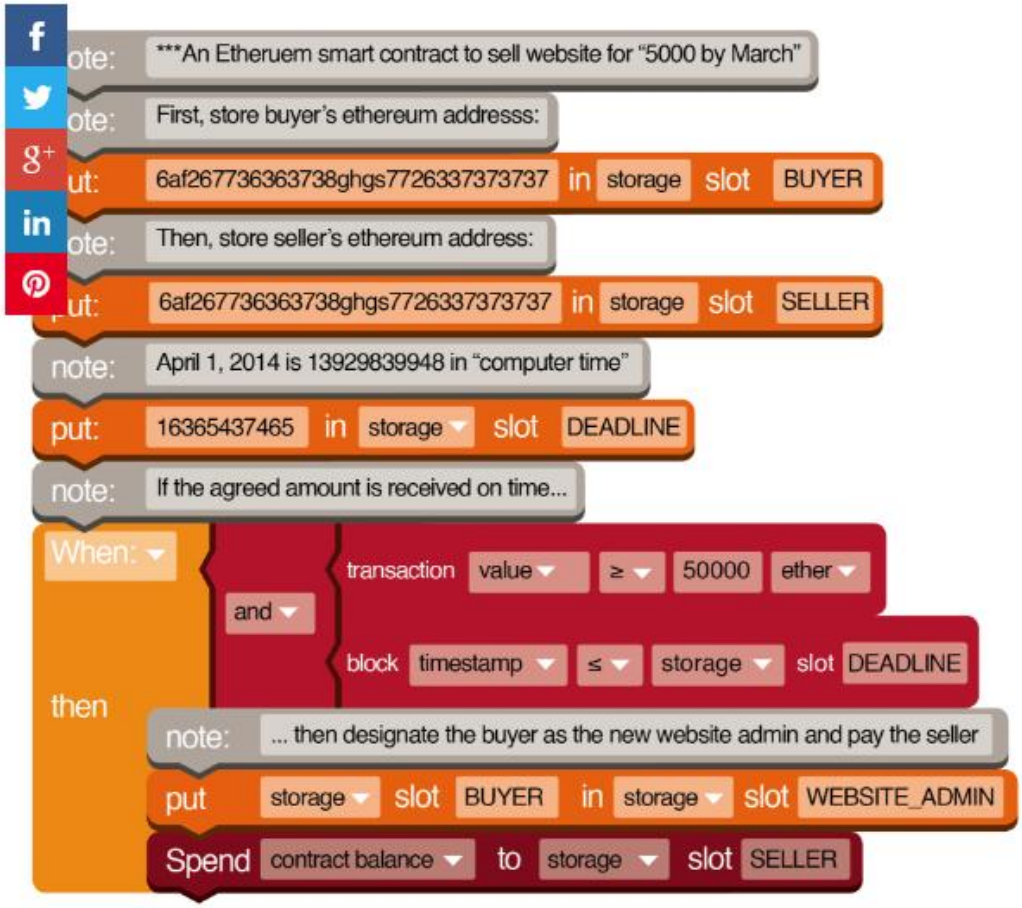


Εικόνα 4: Κώδικας Έξυπνων Συμβόλαιων (Aaron Wright, 2017)

Ο Nick Szabo το 2002 συνέβαλε για ακόμη μία φορά στην ανάπτυξη της των Έξυπνων Συμβολαίων, αναπτύσσοντας ψευδογλώσσα που να μπορεί να διαβάζεται τόσο από ανθρώπους, όσο και από υπολογιστές. Η ειδική αυτή γλώσσα έχει βασικό σκοπό την κατάρτιση κοινών τύπων ιδιωτικών συμφωνητικών και τον ορισμό όρων συμβολαίων, με τρόπο περιεκτικό και σαφή. Οι σχετικές εφαρμογές περιλαμβάνουν οικονομικές συμφωνίες, διαφόρων ειδών αξιόγραφα όπως τίτλους ιδιοκτησίας ή πνευματικά δικαιώματα αλλά και τις μετρήσεις απόδοσης παρεχόμενων υπηρεσιών ή της ροής μιας εφοδιαστικής αλυσίδας. Ουσιαστικά, η ψευδογλώσσα γεφυρώνει το χάσμα μεταξύ της νομικής ορολογίας και του διαδικαστικού κώδικα και ο Szabo με τον τρόπο αυτό επιτυγχάνει την σύγκλιση της ταχύτητας των υπολογιστών και της περιγραφικής δύναμης της ανθρώπινης γλώσσας.

Οι γλώσσες που χρησιμοποιούνται σήμερα για την ανάπτυξη Έξυπνων Συμβολαίων έχουν τις ρίζες τους στις πρώιμες προσπάθειες του Szabo, αλλά η τάση πλέον είναι να ενισχύεται η γραφική απεικόνιση του κώδικα – όπως συμβαίνει και στην περίπτωση

του πρωτοκόλλου του Ethereum. Η γλώσσα του πρωτοκόλλου αυτού, που λέγεται EtherScript, απεικονίζεται σε διαβαθμισμένες, χρωματιστές γραμμές κώδικα. Με τον τρόπο αυτό, ο κώδικας καθίσταται περισσότερο ευανάγνωστος και ευκολονόητος από τους ανθρώπινους χρήστες, όπως στο παράδειγμα συμφωνητικού πώλησης που ακολουθεί:



Source: "What is Ethereum?" EtherScripter, 2016, accessed January 7, 2016

Εικόνα 5: Έξυπνο Συμβόλαιο σε EtherScript (EtherScripter.com)

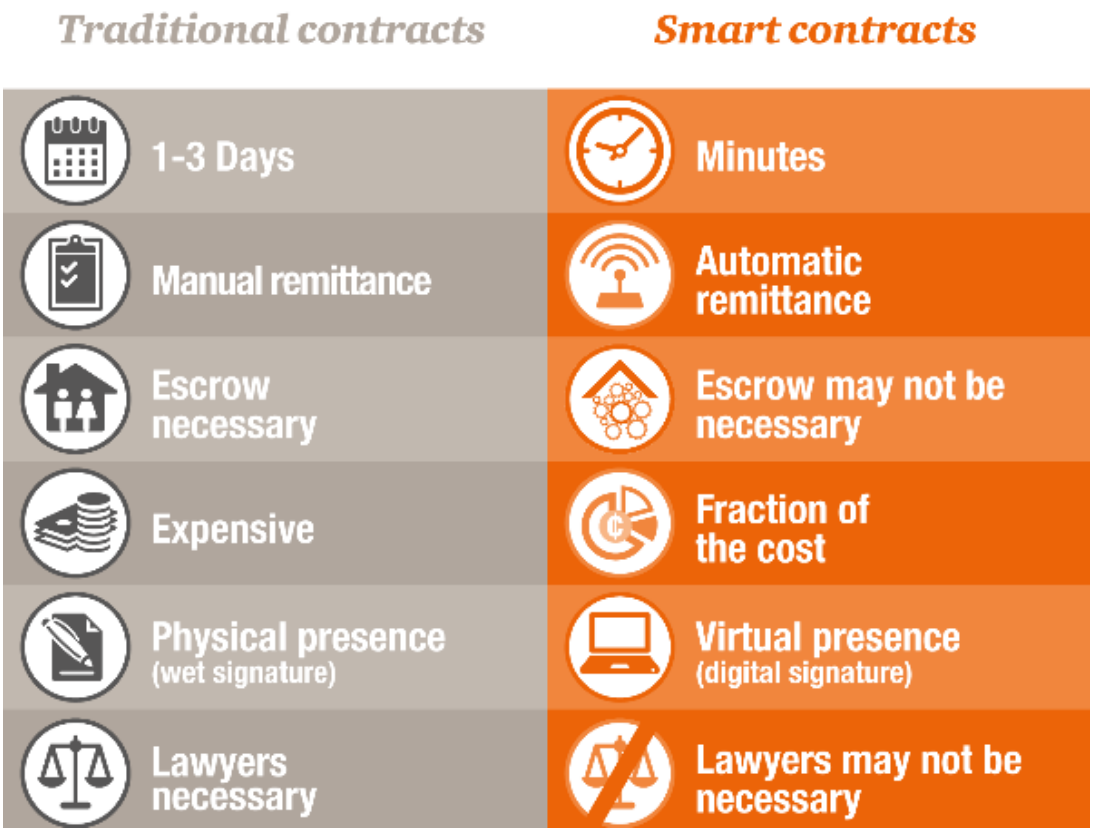
2.3.3 Το ηλεκτρονικό εμπόριο ως πρόδρομος των Έξυπνων Συμβολαίων

Οι επιχειρήσεις Ηλεκτρονικού Εμπορίου, στην προσπάθειά τους να διευκολύνουν τις συναλλαγές με τους πελάτες τους έχουν εδώ και χρόνια ενσωματώσει στις ιστοσελίδες τους διαδικασίες που βασίζονται ουσιαστικά σε εμπορικές συμφωνίες, τους όρους όμως των οποίων μπορεί να ορίζει μόνο το ένα από τα συναλλασσόμενα μέρη. Οι περισσότεροι χρήστες είναι ήδη εξοικειωμένοι με τους Όρους Χρήσης των Ηλεκτρονικών Καταστημάτων. Οι όροι αυτοί δεν είναι καθόλου ευέλικτοι αλλά στη γενική περίπτωση είναι υπέρ αρκετοί, ειδικά για τις περιπτώσεις συναλλαγών σχετικά μικρής αξίας και μάλιστα με αναγνωρισμένους προμηθευτές. Στο Ηλεκτρονικό Εμπόριο όπως εφαρμόζεται μέχρι σήμερα, οι προμηθευτές έχουν πλήρη έλεγχο του περιεχομένου των όρων κάθε εμπορικής συμφωνίας – αφού ο πελάτης πρέπει να συμφωνεί με τους Όρους Χρήσης του καταστήματος και σε άλλη περίπτωση δεν μπορεί να πραγματοποιήσει καμία συναλλαγή με αυτό. Στην περίπτωσή μας λοιπόν, τα συναλλασσόμενα μέρη μπορούν να έχουν έλεγχο κάθε συναλλαγής μέχρι κάποιο μόνο σημείο, αφού οι έμποροι βασίζονται στην αξιοπιστία των χρηματοπιστωτικών ιδρυμάτων που μέσω των πιστωτικών καρτών εγγυώνται την τελική πληρωμή του πελάτη, ο οποίος αναγκαστικά βασίζεται στην πίστη του στο συγκεκριμένο κατάστημα και όσα αναγράφονται στην ιστοσελίδα του για να πραγματοποιήσει την αγορά.

2.3.4 Paper-plus-code contracts – Ένα Υβριδικό Μοντέλο

Όπως έχει προαναφερθεί, συνήθως οι συμφωνίες επικυρώνονται μέσω της έγγραφης καταγραφής των όρων τους σε νομικά κείμενα ή άλλα είδη ειδικών εγγράφων. Μέσω της τεχνολογίας blockchain, είναι δυνατή πλέον η ανάπτυξη εφαρμογών που να

μπορούν να επικυρώνουν και να εκδίδουν τέτοια έγγραφα. Μέσω του κώδικα, οι όροι της συμφωνίας μπορούν να διατυπωθούν επακριβώς σε γλώσσα μηχανής, ενώ παράλληλα εκδίδεται και καταγράφεται ένα αντίγραφο σε μορφή εγγράφου – το οποίο μπορεί να ανακληθεί σε περιπτώσεις παραβίασης των όρων του συμβολαίου από κάποιο/α μέρος/η ή ακόμη και για χρήση σε δικαστήριο. Στην περίπτωση αυτή αναφερόμαστε με τον όρο Υβριδικά Συμβόλαια paper-plus-code. Ο πίνακας που ακολουθεί περιγράφει ορισμένα από τα πολυάριθμα πιθανά πλεονεκτήματα αντίστοιχων εφαρμογών σε σχέση με τα παραδοσιακά συμβόλαια:



Εικόνα 6: Πλεονεκτήματα Έξυπνων Συμβολαίων (Alan Morrison, 2016)

2.4 Βασικές έννοιες στο Ethereum

Ethereum Virtual Machine (EVM): Ethereum Virtual Machine ή EVM είναι το περιβάλλον στο οποίο εκτελούνται οι εφαρμογές Έξυπνων Συμβολαίων στην

πλατφόρμα του Ethereum. Το περιβάλλον είναι σαφώς ορισμένο και πλήρως απομονωμένο, αφού ο κώδικας που εκτελείται στο EVM δεν έχει πρόσβαση στο δίκτυο, αλλά ούτε στα αρχεία συστήματος του υπολογιστή ή κάθε άλλη διαδικασία που εκτελείται παράλληλα. Ακόμη και ανάμεσα σε δύο Έξυπνα Συμβόλαια, η πρόσβαση είναι περιορισμένη.

Gas (αέριο): Για την εκτέλεσή της, κάθε συναλλαγή στην πλατφόρμα του Ethereum απαιτείται συγκεκριμένο αντίτιμο, που μετράται σε μονάδες αερίου οι οποίες αντιστοιχούν σε μονάδες Ether – του έμφυτου κρυπτονομίσματος στην πλατφόρμα Ethereum. Κάθε δημοσίευση ή κατάργηση Έξυπνου Συμβολαίου στο Blockchain απαιτεί επίσης αντίτιμο σε μορφή αερίου. Η κατανάλωση αερίου για τους λόγους που αναλύθηκαν παραπάνω εξυπηρετεί ως αντίτιμο για τις υπηρεσίες των χρηστών που καταναλώνουν επεξεργαστική ισχύ για την καταγραφή των δεδομένων στα μπλοκ. Παράλληλα όμως, μέσω της κατανάλωσης αερίου αποφεύγονται φαινόμενα ατέρμονης εκτέλεσης συμβολαίων στο Ethereum – που θα οδηγούσαν σε κορεσμό του δικτύου.

Accounts (Λογαριασμοί): Υπάρχουν δύο ειδών λογαριασμοί στην πλατφόρμα του Ethereum:

- Εξωτερικά ελεγχόμενοι λογαριασμοί, οι οποίοι ελέγχονται μέσω κρυπτογραφικών κλειδιών – δηλαδή από ανθρώπινους χρήστες. Είναι το μόνο είδος λογαριασμών που μπορεί να εκτελεί συναλλαγές.
- Λογαριασμοί Συμβολαίων, οι οποίοι ελέγχονται από κώδικα και η διεύθυνση των οποίων ορίζεται κατά την δημιουργία του Συμβολαίου.

Transactions (Συναλλαγές): Μία συναλλαγή αποτελεί ουσιαστικά ένα μήνυμα το οποίο αποστέλλεται από ένα Λογαριασμό σε κάποιο άλλο Λογαριασμό. Τα μηνύματα

αυτά μπορούν να περιέχουν γραμμές κώδικα – που αποτελούν το ωφέλιμο φορτίο του μηνύματος – και μονάδες Ether, που αποτελούν το προς μεταφορά ποσό της συναλλαγής. Ο κώδικας εκτελείται στο EVM και τα αποτελέσματά του καταγράφονται στην αλυσίδα των μπλοκ. Οι συναλλαγές μεταβάλλουν την αλυσίδα των μπλοκ και όπως έχει προαναφερθεί, κάθε συναλλαγή για την εκτέλεσή της απαιτεί την κατανάλωση μονάδων αερίου.

Message Calls (Κλήσεις Μηνυμάτων): Τα Συμβόλαια επικοινωνούν μεταξύ τους μέσω των Κλήσεων Μηνυμάτων (αφού όπως έχει προαναφερθεί, μόνο οι εξωτερικά ελεγχόμενοι λογαριασμοί μπορούν να πραγματοποιούν συναλλαγές και να εκτελούν κώδικα Συμβολαίων). Οι Κλήσεις Μηνυμάτων δεν επηρεάζουν τη δομή της αλυσίδας των μπλοκ και άρα, δεν καταναλώνουν καθόλου αέριο. Ουσιαστικά αποτελούν την μέθοδο επίκλησης Συμβολαίων από άλλα Συμβόλαια, εντός του EVM.

2.5 Decentralized Applications (dApps)

Τα Decentralized Applications (dApps) είναι κατανεμημένες εφαρμογές, υπό την έννοια ότι είναι εφαρμογές που εκτελούνται σε ένα Peer-to-Peer (P2P) δίκτυο υπολογιστών και όχι σε ένα μόνο υπολογιστή.

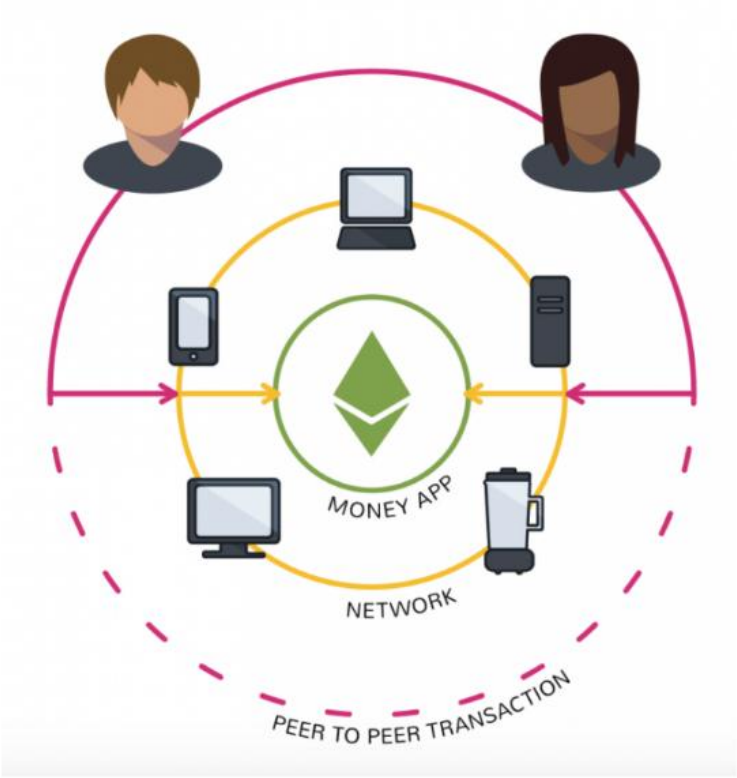
Στη Λεύκη Βίβλο του Ethereum (Ethereum White Paper) γίνεται διαχωρισμός των dApps σε τρεις κατηγορίες:

1. Η πρώτη κατηγορία αφορά χρηματοοικονομικές εφαρμογές, όπου ουσιαστικά η εφαρμογή διαχειρίζεται κάποιο χρηματικό ποσό και μόνον. Ένα παράδειγμα εφαρμογής θα μπορούσε να είναι ένα πορτοφόλι αποταμίευσης.
2. Η δεύτερη κατηγορία αφορά εφαρμογές όπου εμπλέκεται η μεταφορά χρηματικών ποσών μεταξύ κόμβων, αλλά παράλληλα η εφαρμογή εξυπηρετεί

και κάποιο άλλο σκοπό. Ένα παράδειγμα θα μπορούσε να είναι μια εφαρμογή που αυτόματα μεταφέρει αμοιβές σε χρήστες για την επίλυση υπολογιστικών προβλημάτων

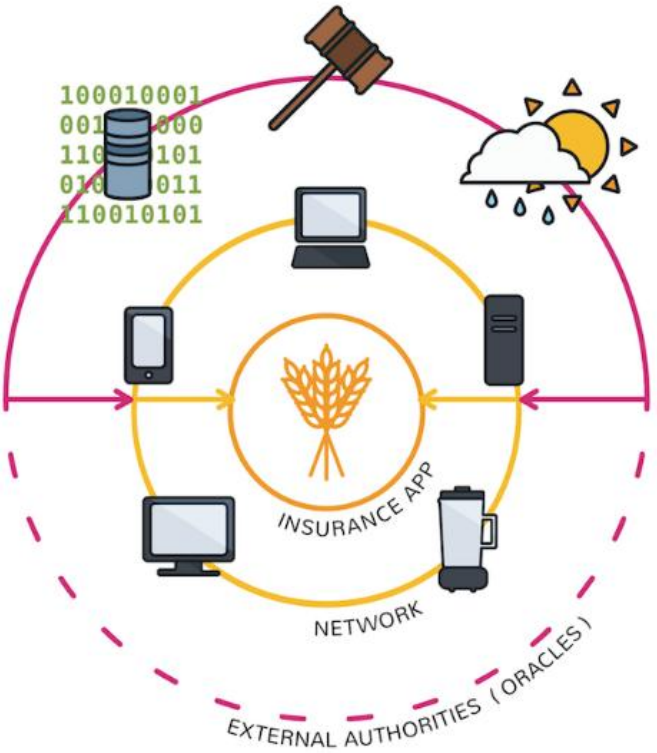
3. Η Τρίτη κατηγορία αφορά εφαρμογές που δεν σχετίζονται με μεταφορά χρημάτων όπως για παράδειγμα εφαρμογές για ψηφοφορία μέσω δικτύου, συστήματα αποκεντρωμένης διακυβέρνησης κ.α.

Όσον αφορά την πρώτη κατηγορία, ένα περισσότερο αναλυτικό παράδειγμα θα μπορούσε να αποτελεί η περίπτωση που ένας χρήστης χρειάζεται να μεταφέρει μονάδες ETH για να ενεργοποιήσει ένα Έξυπνο Συμβόλαιο με κάποιον άλλο χρήστη, χρησιμοποιώντας τους κόμβους του δικτύου για την μεταφορά των δεδομένων, όπως φαίνεται και στο ακόλουθο διάγραμμα:



Εικόνα 7: Πρώτη κατηγορία dApps (Maria Kuznetsov)

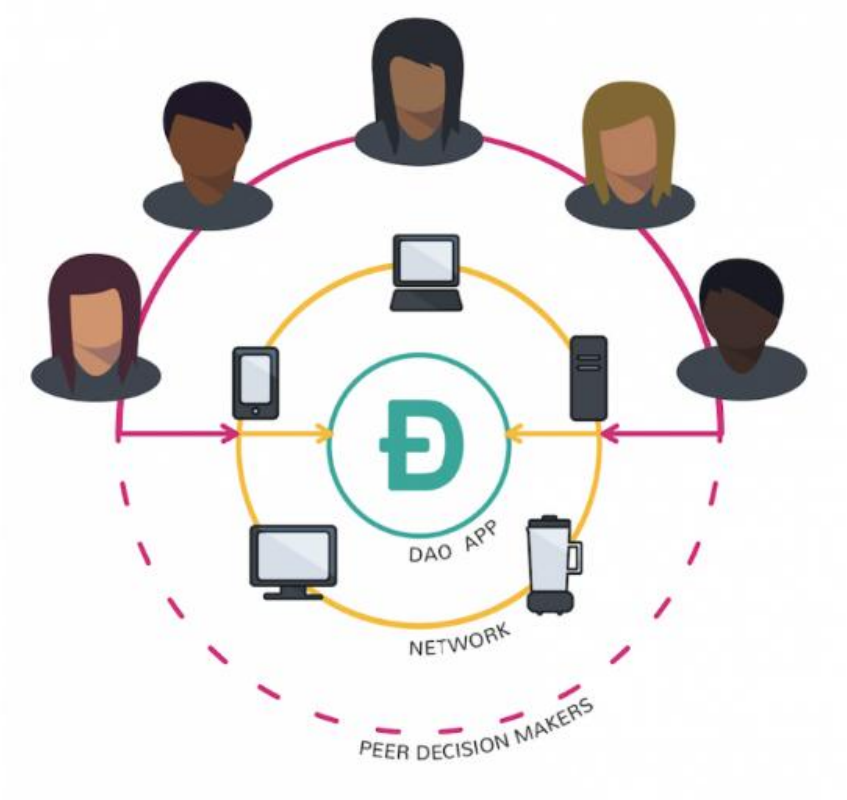
Όσον αφορά την δεύτερη κατηγορία - όπου η εφαρμογή εμπλέκεται τόσο με μεταφορά αξίας όσο και με επεξεργασία πληροφοριών που προέρχονται εκτός της αλυσίδας των μπλοκ - ένα περισσότερο αναλυτικό παράδειγμα θα μπορούσε να αποτελεί η περίπτωση όπου μια εφαρμογή σχετική με την ασφάλιση αγροτικής σοδειάς, θα έπρεπε να είναι συνδεδεμένη με μια ιστοσελίδα μετεωρολογικών προβλέψεων, από όπου θα αντλούσε δεδομένα για τον καιρό ώστε να αποφασιστεί εάν κάποιος χρήστης δικαιούται αποζημίωση, όπως φαίνεται και στο ακόλουθο διάγραμμα:



Εικόνα 8: Δεύτερη κατηγορία dApps (Maria Kuznetsov)

Στο σημείο αυτό σημειώνουμε πως οι οργανισμοί από τους οποίους εξαρτώνται τα Έξυπνα Συμβόλαια για να αντλούν πληροφορίες πραγματικού χρόνου για το περιβάλλον ονομάζονται “oracles” (ελληνικά: «προφήτες»)

Όσον αφορά την τρίτη κατηγορία, ένα περισσότερο αναλυτικό παράδειγμα θα μπορούσε να αποτελεί η περίπτωση ενός DAO (όπως θα αναλυθεί στη συνέχεια), όπου υπάρχουν σαφείς κανόνες για τις αποφάσεις που θα ληφθούν βάσει ψηφοφορίας των μελών, όπως φαίνεται και στο ακόλουθο διάγραμμα:



Εικόνα 9: Τρίτη κατηγορία dApps (Maria Kuznetsov)

Στο σημείο αυτό αξίζει να αναφερθούμε στο γεγονός ότι, η διαδικασία δημιουργίας ενός dApp μπορεί να περιλαμβάνει τη διοργάνωση ενός ICO (όπως θα αναλυθεί στη συνέχεια), για την συγκέντρωση Κεφαλαίων που θα υποστηρίξουν οικονομικά το εγχείρημα.

2.6 Initial Coin Offerings (ICOs)

Οι νεοφυείς επιχειρήσεις που σχετίζονται με την τεχνολογία Blochchain και αναζητούν πηγές χρηματοδότησης, έχουν πλέον την επιλογή να οργανώσουν ένα

«Initial Coin Offering", ή όπως συχνότερα αποκαλείται, ένα ICO. Αντί να λάβουν χρηματοδότηση από κάποιο fund με αντάλλαγμα ορισμένο ποσοστό συμμετοχής, οι εταιρίες αυτές εκδίδουν το δικό τους ψηφιακό νόμισμα, που οποιοσδήποτε μπορεί να προμηθευτεί σε ένα crowdsale. Τα κέρδη από την δημοπράτηση αυτών των ψηφιακών «μετοχών» βοηθούν τις εταιρίες που τις εκδίδουν με την χρηματοδότηση της επιχειρηματικής τους δραστηριότητας.

Η διαδικασία έχει αρκετές ομοιότητες με την Αρχική Δημόσια Προσφορά (ΑΔΠ) των μετοχών κάποιας εταιρίας στο χρηματιστήριο, με τη διαφορά πως ενώ η διαδικασία της ΑΔΠ είναι αυστηρά καθορισμένη και υποστηριζόμενη από κυβερνήσεις, το πεδίο με τα ICOs είναι ακόμη θολό. Η επιτροπή Κεφαλαιαγοράς των Ηνωμένων Πολιτειών Αμερικής καθώς και άλλοι ρυθμιστικοί οργανισμοί ερευνούν ήδη τα χαρακτηριστικά των σχετικών εφαρμογών, ενώ οι υποστηρικτές των ICOs υποστηρίζουν πως τα ICOs είναι ένα εργαλείο που μπορεί να φέρει επανάσταση όχι απλά στην αγορά συναλλάγματος, αλλά και σε ολόκληρο το χρηματοπιστωτικό σύστημα – αφού τα ειδικά ψηφιακά νομίσματα που εκδίδουν οι εταιρίες μπορούν να γίνουν τα αξιόγραφα και οι μετοχές του αύριο (Blockgeeks.com).

2.6.1 Σύντομη αναδρομή της ιστορίας των ICOs

Πιθανότατα το πρώτο ψηφιακό νόμισμα που εκδόθηκε στα πλαίσια διαδικασίας ICO είναι το Ripple. Στις αρχές του 2013 τα Ripple Labs ανέπτυξαν το σύστημα πληρωμών που ονομάστηκε Ripple και στα πλαίσια αυτού του εγχειρήματος εκδόθηκαν περίπου 100 δισεκατομμύρια ψηφιακές μονάδες νομίσματος XRP. Η εταιρία πούλησε αυτές τις μονάδες για να χρηματοδοτήσει την ανάπτυξη της πλατφόρμας Ripple.

Αργότερα το 2013, μέσω του Mastercoin (που πλέον ονομάζεται Omni) - ενός ψηφιακού νομίσματος και πρωτοκόλλου επικοινωνιών που βασίστηκε στο Blockchain του Bitcoin - έγιναν προσπάθειες να δημιουργηθεί ένα επιπλέον επίπεδο στην πλατφόρμα Bitcoin για να εκτελούνται έξυπνα συμβόλαια και να εκδοθούν ειδικές ψηφιακές μονάδες για ανταλλαγή με Bitcoin. Οι υπεύθυνοι ανάπτυξης ανταλλάξανε κάποια εκατομμύρια ψηφιακές μονάδες Mastercoin με Bitcoin και με αυτό τον τρόπο συγκεντρώσανε αξία ενός εκατομμύριου δολαρίων Η.Π.Α.

Αρκετά ακόμη κρυπτονομίσματα έχουν χρηματοδοτηθεί μέσω ICO, αλλά σίγουρα αυτό που συγκεντρώνει το περισσότερο ενδιαφέρον είναι το Ethereum. Στα μέσα του 2014 το ίδρυμα Ethereum πούλησε τα ψηφιακά νομίσματα που έκδωσε και ονομάστηκαν Ether (ETH), με αντάλλαγμα 0.0005 Bitcoin για κάθε μονάδα Ether. Με αυτόν τον τρόπο, συγκεντρώθηκαν σχεδόν είκοσι εκατομμύρια Δολάρια, το μεγαλύτερο ποσό που συγκεντρώθηκε ποτέ μέσω crowdfunding και χρησιμοποιήθηκε για την Κεφαλαιακή βάση της ανάπτυξης του Ethereum. Καθώς το Ethereum αυτό καθαυτό εισήγαγε την έννοια των Έξυπνων συμβολαίων, άνοιξε το δρόμο για τη νέα γενιά των ICO.

2.6.2 Το Ethereum ως εργαλείο ICO crowdfunding

Μια από τις απλούστερες εφαρμογές του συστήματος Έξυπνων συμβολαίων του Ethereum είναι η δημιουργία ειδικών ψηφιακών νομισμάτων, με τα οποία μπορούν να πραγματοποιηθούν συναλλαγές στο Blockchain του Ethereum – αντί για συναλλαγές με Ether.

Απόδειξη των δυνατοτήτων των Έξυπνων Συμβολαίων του Ethereum υπήρξε σίγουρα η εταιρία The DAO, ένας κατανεμημένος αυτόνομος οργανισμός με σκοπό την παροχή ενός νέου αποκεντρωμένου επιχειρηματικού μοντέλου για την οργάνωση

τόσο επιχειρήσεων όσο και Μη Κερδοσκοπικών Οργανισμών, που βασίστηκε στο Blockchain του Ethereum και δεν είχε κεντρική διοίκηση. Μέσω ICO, η The DAO συγκέντρωσε Ether αξίας εκατό εκατομμυρίων Δολαρίων. Η έννοια του Κατανεμημένου Αυτόνομου Οργανισμού (Distributed Autonomous Organization – DAO) θα αναλυθεί στην επόμενη ενότητα.

Η ιδέα της χρηματοδότησης επιχειρηματικών εγχειρημάτων μέσω των ειδικών ψηφιακών μονάδων που εκδίδονται από Έξυπνα Συμβόλαια στην πλατφόρμα του Ethereum, έγινε πρότυπο για μια νέα γενιά επιτυχημένων εγχειρημάτων Crowdfunding. Ενδεικτικά αναφέρουμε ορισμένα παραδείγματα:

- Augur
- Melonport
- Golem
- ICONOMI
- Singular DTV
- First Blood
- Digix DAO.

2.7 Distributed Autonomous Organization (DAO)

Η τεχνολογία των αλυσίδων από μπλοκ επιτρέπει την εκτέλεση και διασύνδεση διαφόρων Έξυπνων Συμβολαίων, τα οποία αλληλεπιδρούν μεταξύ τους με τρόπο αποκεντρωμένο και διαμοιρασμένο. Πολλαπλά Έξυπνα Συμβόλαια μπορούν να συνδυαστούν με τρόπο ώστε να σχηματίσουν Κατανεμημένους Οργανισμούς, η λειτουργία των οποίων βασίζεται σε συγκεκριμένους κανόνες και διαδικασίες, όπως ορίζονται από τον κώδικα των Έξυπνων αυτών Συμβολαίων.

Μέσω ενός Κατανεμημένου Οργανισμού βασισμένου στην τεχνολογία της αλυσίδας των μπλοκ, άνθρωποι και μηχανές (ή ένας συνδυασμός αυτών) μπορούν να συντονίζουν τις κινήσεις τους διαμέσου ενός συνόλου κωδικοποιημένων Έξυπνων Συμβολαίων, χωρίς να ενσωματωθούν σε μια παραδοσιακή επιχειρηματική οντότητα. Η διακυβέρνηση ενός τέτοιου οργανισμού μπορεί να επιτευχθεί μέσω της καταγραφής των συναλλαγών απευθείας σε μια αλυσίδα από μπλοκ. Χαρακτηριστικά από παραδοσιακά μοντέλα διακυβέρνησης επιχειρήσεων είναι επίσης δυνατόν να ενσωματωθούν στη διαδικασία, μέσω του διαμοιρασμού της ικανότητας λήψης αποφάσεων σε πολλαπλά μέρη του οργανισμού με χρήση τεχνολογίας πολλαπλών υπογραφών (multiple signature (multi-sig) technology), αποτρέποντας με αυτό τον τρόπο το σύστημα από την εκτέλεση κάποιας ενέργειας, χωρίς την συγκατάθεση όλων των ενδιαφερομένων μερών.

Σε αντίθεση με τους παραδοσιακούς οργανισμούς, όπου η ικανότητα λήψης αποφάσεων συγκεντρώνεται στην κορυφή του οργανογράμματος, σε ένα Κατανεμημένο Οργανισμό η ικανότητα αυτή μπορεί να κωδικοποιηθεί και να ενσωματωθεί απευθείας στο κώδικα των Έξυπνων Συμβολαίων. Οι μέτοχοι μπορούν να συμμετέχουν στην διαδικασία λήψης αποφάσεων μέσω κατανεμημένων ψήφων, διαμοιράζοντας με τον τρόπο αυτό την εξουσία στα μέρη που απαρτίζουν τον οργανισμό, χωρίς την ανάγκη ύπαρξης κεντρικού ελέγχου από κάποια αρχή (όπως το Διοικητικό Συμβούλιο ενός παραδοσιακού οργανισμού).

Καθώς η σχετική τεχνολογία εξελίσσεται, καθίσταται δυνατή η σύσταση Κατανεμημένων Αυτόνομων Οργανισμών, οι οποίοι μπορούν να αναπτύσσουν σχέσεις - βάσει Έξυπνων Συμβολαίων - με ανθρώπους και μηχανές. Σκοπός είναι η δημιουργία ενός σύνθετου οικοσυστήματος από αυτόνομους αντιπροσώπους, οι

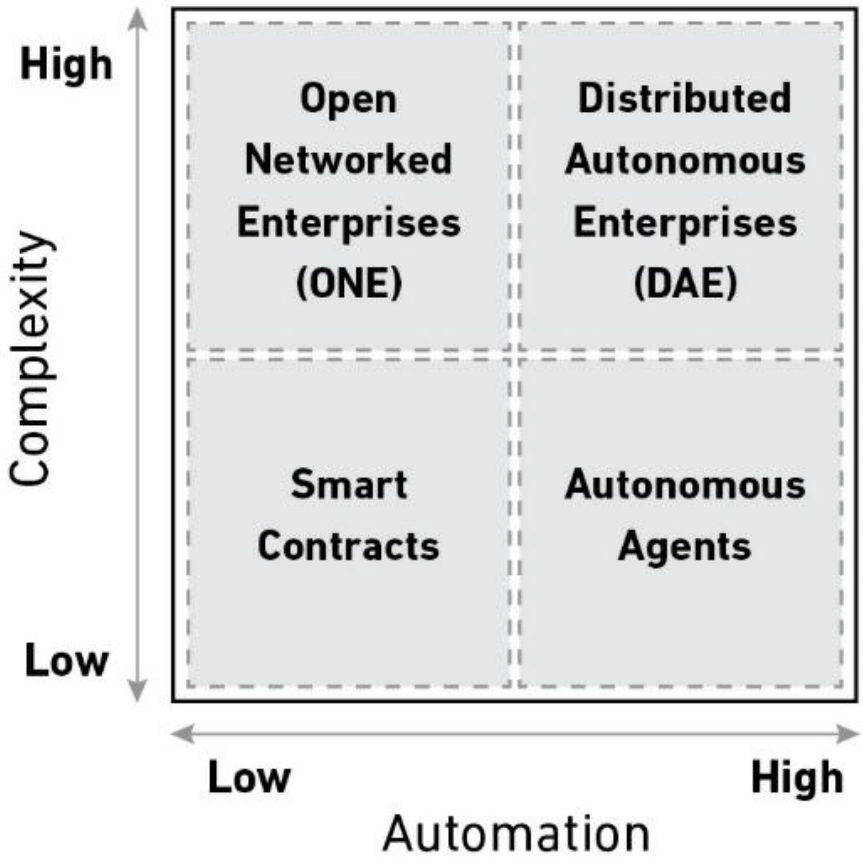
οποίοι αλληλεπιδρούν μεταξύ τους σύμφωνα με ένα σύνολο προκαθορισμένων και αυτόματα εκτελούμενων κανόνων.

Οι Κατανεμημένοι Αυτόνομοι Οργανισμοί είναι ουσιαστικά Κατανεμημένοι Οργανισμοί οι οποίοι είναι τόσο αυτόνομοι (με την έννοια ότι, αφότου έχουν αναπτυχθεί εντός της αλυσίδας των μπλοκ, λειτουργούν αυτόνομα και χωρίς την παρουσία ή τον έλεγχο των δημιουργών τους), όσο και αυτάρκεις (με την έννοια ότι έχουν την δυνατότητα να συγκεντρώνουν Κεφάλαια, όπως ψηφιακά νομίσματα ή φυσικά περιουσιακά στοιχεία). Οι Κατανεμημένοι Αυτόνομοι Οργανισμοί μπορούν να χρεώνουν τους χρήστες για τις υπηρεσίες που τους παρέχουν, ώστε με τη σειρά τους να μπορούν να εξοφλούν τρίτους για τους πόρους που απαιτούνται για τη λειτουργία τους. Για το χρονικό διάστημα που οι οργανισμοί αυτοί μπορούν να συγκεντρώνουν επαρκείς πόρους για την αυτόνομη λειτουργία τους, μπορούν να υφίστανται χωρίς να βασίζονται σε κάποιον τρίτο οργανισμό.

Ένας Κατανεμημένος Αυτόνομος Οργανισμός που σκοπό έχει να αναζητά χρηματοοικονομικά οφέλη, συνήθως με τη μορφή μερισμάτων, ονομάζεται Κατανεμημένη Αυτόνομη Εταιρεία (Distributed Autonomous Corporation – DAC).

2.7.1 Κατανεμημένες Επιχειρηματικές Οντότητες σύμφωνα με τους Don και Alex Tapscott

Οι Don και Alex Tapscott, στο βιβλίο τους “Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world”, ορίζουν τέσσερις κατηγορίες νέων επιχειρηματικών μοντέλων για Κατανεμημένες Επιχειρηματικές Οντότητες, ανάλογα με τον βαθμό της επιχειρησιακής πολυπλοκότητας που τις διακρίνει και της εμπλοκής ανθρώπων στη λειτουργία τους, σύμφωνα με το ακόλουθο γράφημα:



Εικόνα10 : Κατανεμημένες Επιχειρηματικές Οντότητες (Don Tapscott, Alex Tapscott, 2016)

Ο οριζόντιος άξονας αφορά τον βαθμό συμμετοχής του ανθρώπινου παράγοντα στο εκάστοτε μοντέλο. Στο αριστερό μέρος, το μοντέλο απαιτεί κάποιας μορφής εμπλοκή ανθρώπων, ενώ στο δεξί μέρος το μοντέλο δεν απαιτεί καθόλου ανθρώπινη παρουσία.

Ο κάθετος άξονας αφορά την λειτουργική πολυπλοκότητα κάθε μοντέλου (και όχι την τεχνική πολυπλοκότητα αυτού). Στο κάτω μέρος, τα μοντέλα εκτελούν μία μοναδική λειτουργία, ενώ στην κορυφή τα μοντέλα επιτελούν διάφορες λειτουργίες.

Αναλυτικά για κάθε μοντέλο:

- Smart Contracts: Εάν μελετηθούν αυτόνομα, εμπεριέχουν την λιγότερη πολυπλοκότητα και απαιτούν την λιγότερη ανθρώπινη εμπλοκή.

- Open Networked Enterprises: Χρησιμοποιώντας Έξυπνα Συμβόλαια, επιχειρήσεις μπορούν να συνδυαστούν με άλλες, εντός δικτύου.
- Autonomous Agents: Λιγότερο ή περισσότερο αναπτυγμένες συσκευές ή λογισμικό, που ρυθμίζουν τις ενέργειές τους με σκοπό την επίτευξη συγκεκριμένων στόχων, οι οποίες δεν μπορούν να ελέγχονται από κανέναν, παρά μόνον από την ίδια τη συσκευή (ή λογισμικό).
- Distributed Autonomous Enterprises: Ουσιαστικά το μοντέλο με την περισσότερη πολυπλοκότητα, στο οποίο τα μέρη συμμετέχουν μέσω Έξυπνων Συμβολαίων στην επίτευξη κοινών στόχων και όπου κάθε ενέργεια δεν ενεργοποιείται μόνο από ανθρώπινους χρήστες, αλλά και από κάθε ψηφιακή οντότητα που μπορεί να αλληλεπιδρά με την αλυσίδα των μπλοκ.

ΚΕΦΑΛΑΙΟ 3: HYPERLEDGER PROJECT

3.1 Η ιστορία του Hyperledger Project

Το Δεκέμβριο του 2015, το Ίδρυμα Linux (Linux Foundation) ανακοίνωσε τη δημιουργία του Hyperledger Project *(www.hyperledger.org)*. Σκοπός του εγχειρήματος είναι η ενίσχυση της συνεργασίας μεταξύ εταιρειών διαφόρων κλάδων, μέσω της ανάπτυξης Κατανεμημένων Καθολικών και πλατφορμών Blockchain ανοιχτού κώδικα. Έχει δοθεί ιδιαίτερη σημασία στην βελτίωση της απόδοσης και την αύξηση της αξιοπιστίας των συστημάτων, ώστε να είναι ικανά να υποστηρίξουν επιχειρηματικές συναλλαγές σε παγκόσμιο επίπεδο - συναλλαγές μεταξύ των μεγαλύτερων χρηματοπιστωτικών οργανισμών και πολυεθνικών εταιρειών. Ιδιαίτερη έμφαση έχει επίσης δοθεί σε εφαρμογές για την βελτίωση των διαδικασιών της εφοδιαστικής αλυσίδας.

Το εγχείρημα αποσκοπεί στην σύγκλιση ανεξάρτητων επιμέρους προσπαθειών για την ανάπτυξη ανοιχτών πρωτοκόλλων και standards, παρέχοντας ένα βαθμωτό πλαίσιο ανάπτυξης κώδικα ικανό να υποστηρίξει διαφορετικά στοιχεία συστήματος (components), για διαφορετικές χρήσεις. Περιλαμβάνονται αλυσίδες των μπλοκ με ξεχωριστό μοντέλο κοινής συναίνεσης και διαφορετικές ρουτίνες για αποθήκευση δεδομένων, αλλά και υπηρεσίες για ταυτοποίηση χρηστών, έλεγχο πρόσβασης και Έξυπνα Συμβόλαια.

Στις αρχές του 2016, το Ίδρυμα Linux άρχισε να δέχεται προσφορές για την ενσωμάτωση Πηγαίου Κώδικα και άλλων τεχνολογιών στο εγχείρημα του Hyperledger. Στο σημείο αυτό, αξίζει να γίνει ιδιαίτερη αναφορά στην ενσωμάτωση, αρχικά του εγχειρήματος OpenBlockchain της IBM, που στη συνέχεια ονομάστηκε

Fabric και στη συνέχεια, του εγχειρήματος Κατανεμημένου Καθολικού (Distributed Ledger) της Intel, που ονομάζεται Sawtooth.

Στη συνέχεια, προστέθηκαν πληθώρα εταιρειών στο οικοσύστημα του Hyperledger project, καθώς και αρκετές πλατφόρμες αλυσίδων των μπλοκ, πέραν αυτών της IBM και της Intel, όπως θα αναλυθούν στη συνέχεια.

Ακολούθως παρατίθενται οι εταιρείες μέλη της κοινοπραξίας του Hyperledger project. Είναι σαφές πως στο οικοσύστημα έχουν εισχωρήσει πολλές και μεγάλες πολυεθνικές εταιρείες, από διάφορους κλάδους όπως αυτοί των χρηματοπιστωτικών οργανισμών, εταιρειών τεχνολογίας, πληροφορικής, τηλεπικοινωνιών κ.α.

Εικόνα 11: Hyperledger Consortium (*hyperledger.org*)

3.2 Οι πλατφόρμες Blockchain του Hyperledger Project

Το Hyperledger ενσωματώνει και προωθεί μια σειρά από τεχνολογίες Blockchain για επιχειρήσεις οι οποίες περιλαμβάνουν πλαίσια για Κατανεμημένα Καθολικά (Distributed Ledgers), μηχανές για ανάπτυξη Έξυπνων Συμβολαίων, βιβλιοθήκες εφαρμογών πελάτη, γραφικά περιβάλλοντα και βιβλιοθήκες και δείγματα εφαρμογών. Η στρατηγική ομπρέλας που ακολουθείται ενθαρρύνει την επαναχρησιμοποίηση κοινών δομικών στοιχείων και επιτρέπει την γρήγορη ανάπτυξη τεχνολογιών Κατανεμημένου Καθολικού.

Ακολούθως αναλύονται οι πλατφόρμες Blockchain του Hyperledger Project, ως ισχύουν κατά την περίοδο συγγραφής της παρούσας εργασίας:

Hyperledger Fabric: Σκοπός του Hyperledger Fabric είναι να αποτελεί τη βάση για την ανάπτυξη εφαρμογών ή λύσεων με βαθμωτή αρχιτεκτονική. Ορισμένα δομικά στοιχεία όπως μοντέλα κοινής συναίνεσης, μπορούν να επαναχρησιμοποιηθούν και μάλιστα είναι έτοιμα για σύνδεση και άμεση λειτουργία (plug-and-play). Οι εταιρείες Digital Asset και η IBM, από τις μεγαλύτερες εταιρείες στον χώρο της πληροφορικής, έχει συνεισφέρει την πλατφόρμα Fabric στο οικοσύστημα του Hyperledger.

Hyperledger Sawtooth: Πρόκειται για μια βαθμωτή πλατφόρμα ανάπτυξης Κατανεμημένων Καθολικών (Distributed Ledgers). Το Hyperledger Sawtooth περιλαμβάνει ένα καινοτόμο αλγόριθμο κοινής συναίνεσης (consensus algorithm), που ονομάζεται Proof of Elapsed Time (PoET) και στοχεύει σε ιδιαίτερα μεγάλους πληθυσμούς χρηστών για την επιβεβαίωση των μπλοκ και χαρακτηρίζεται από την ελάχιστη δυνατή κατανάλωση επεξεργαστικών πόρων. Η Intel, η μεγαλύτερη εταιρεία παραγωγής επεξεργαστών, έχει συνεισφέρει την πλατφόρμα Sawtooth στο οικοσύστημα του Hyperledger.

Hyperledger Iroha: Πρόκειται για ένα πλαίσιο ανάπτυξης αλυσίδων από μπλοκ για επιχειρήσεις, σχεδιασμένο για εύκολη και γρήγορη ενσωμάτωση σε έργα υποδομής που απαιτούν τεχνολογία Κατανεμημένων Καθολικών. Ιδιαίτερη έμφαση έχει δοθεί στην ανάπτυξη εφαρμογών για περιβάλλοντα Mobile. Οι εταιρείες Soramitsu, Hitachi, NTT Data και Colu είναι αυτές που αρχικά συνεισφέρανε το Iroha στο οικοσύστημα του Hyperledger.

Hyperledger Burrow: Πρόκειται για ένα περιβάλλον Έξυπνων Συμβολαίων με εξουσιοδότηση. Το Burrow, που ανακοινώθηκε το 2014, υπήρξε η πρώτη πλατφόρμα

του είδους του. Παρέχεται μια εφαρμογή πελάτη βαθμωτού τύπου, που χαρακτηρίζεται από μια μηχανή Έξυπνων Συμβολαίων με εξουσιοδότηση, με χαρακτηριστικά σύμφωνα με τις προδιαγραφές του Ethereum Virtual Machine (EVM). Η εταιρεία Monax έχει αρχικά συνεισφέρει την πλατφόρμα Burrow στο οικοσύστημα του Hyperledger και το εγχείρημα συγχρηματοδοτήθηκε από την Intel.

Hyperledger Indy: Η εν λόγω πλατφόρμα παρέχει εργαλεία, βιβλιοθήκες και επιμέρους στοιχεία συστήματος που μπορούν να επαναχρησιμοποιηθούν. Σκοπός του εγχειρήματος είναι η καταγραφή ψηφιακών ταυτοτήτων σε αλυσίδες από μπλοκ ή άλλα Κατανεμημένα Καθολικά, ώστε να είναι δυνατή η αλληλεπίδραση μεταξύ εφαρμογών σε διάφορα περιβάλλοντα. Το εγχείρημα την χρονική στιγμή συγγραφής της παρούσας εργασίας βρίσκεται υπό ανάπτυξη.

3.3 Η εργαλειοθήκη του Hyperledger Project

Hyperledger Cello: Πρόκειται ουσιαστικά για μια βαθμωτή εργαλειοθήκη για αλυσίδες από μπλοκ. Σκοπός του Cello είναι η εφαρμογή του κατά παραγγελία μοντέλου "as-a-service" στο οικοσύστημα των αλυσίδων από μπλοκ, ώστε να ελαχιστοποιηθεί η προσπάθεια που απαιτείται για τη δημιουργία, τη διαχείριση και τον τερματισμό λειτουργίας αλυσίδων από μπλοκ. Το Hyperledger Cello έχει συνεισφέρει στο οικοσύστημα του Hyperledger Project η IBM, με συγχρηματοδότηση από τις Soramitsu, Huawei και Intel.

Hyperledger Composer: Πρόκειται μια ομάδα εργαλείων για την ανάπτυξη εταιρικών δικτύων βασισμένων σε τεχνολογία αλυσίδας των μπλοκ. Σκοπός του Composer είναι να διευκολύνει την ανάπτυξη Έξυπνων Συμβολαίων και εφαρμογών Blockchain από προγραμματιστές για επιχειρηματίες που επιθυμούν να επιλύσουν επιχειρησιακά προβλήματα.

Hyperledger Explorer: Έχει σχεδιαστεί για τη δημιουργία μια Web εφαρμογής φιλικής προς τον χρήστη. Ο Hyperledger Blockchain Explorer μπορεί να προσπελάσει μπλοκ, συναλλαγές, πληροφορίες για τους κόμβους του δικτύου, καθώς και κάθε σχετική πληροφορία που έχει καταγραφεί στο καθολικό. Οι εταιρείες IBM, Intel DTC έχουν συνεισφέρει τον Explorer στο οικοσύστημα του Hyperledger Project.

Hyperledger Quilt: Είναι ένα εργαλείο που παρέχει διαλειτουργικότητα μεταξύ συστημάτων ανάπτυξης Καθολικών μέσω της εφαρμογής του ILP. Το ILP είναι ένα πρωτόκολλο συναλλαγών που έχει σχεδιαστεί για τη μεταφορά αξίας μεταξύ Κατανεμημένων και παραδοσιακών Καθολικών. Το εγχείρημα την χρονική στιγμή συγγραφής της παρούσας εργασίας βρίσκεται υπό ανάπτυξη.

ΚΕΦΑΛΑΙΟ 4: R3 CORDA

4.1 Παρουσίαση του R3 CORDA

Το Corda είναι μια πλατφόρμα ανάπτυξης Κατανεμημένων Καθολικών (Distributed Ledgers), σχεδιασμένη για την καταγραφή και διαχείριση χρηματοοικονομικών συμφωνιών μεταξύ συστημικών χρηματοπιστωτικών οργανισμών. Το Corda είναι εμπνευσμένο από τα συστήματα Blockchain και ενσωματώνει αρκετά από τα χαρακτηριστικά τους, πλην όμως αυτών που καθιστούν τα Blochains ακατάλληλα για εφαρμογές του χρηματοπιστωτικού τομέα.

Τα κύρια χαρακτηριστικά της πλατφόρμας Corda περιλαμβάνουν:

- Στο Corda δεν γίνεται διαμοιρασμός των πληροφοριών σε όλους τους κόμβους του δικτύου – μόνο τα ενδιαφερόμενα μέρη με νόμιμο δικαίωμα στη γνώση της σχετικής πληροφορίας μπορούν να έχουν πρόσβαση στα χαρακτηριστικά μιας συμφωνίας.
- Η πλατφόρμα Corda διαχειρίζεται την ροή εργασιών ανάμεσα σε εταιρείες, χωρίς όμως την παρουσία κάποιου κεντρικού μηχανισμού ελέγχου.
- Στο Corda επιτυγχάνεται κοινή συναίνεση μεταξύ των εταιρειών που συμμετέχουν μόνο στο επίπεδο κάθε συμφωνίας που συνάπτουν, και όχι σε επίπεδο συστήματος.
- Η δομή του Corda επιτρέπει την δημιουργία κόμβων του δικτύου με ρόλο επιτηρητή, για την επίβλεψη της λειτουργίας του συστήματος αλλά και για λόγους ρυθμιστικούς.
- Στην πλατφόρμα Corda, κάθε συναλλαγή επιβεβαιώνεται μόνο από τα μέρη που συμμετέχουν σε αυτή και όχι από όλους τους κόμβους του δικτύου.
- Η πλατφόρμα Corda υποστηρίζει πληθώρα μηχανισμών κοινής συναίνεσης.

- Στο Corda γίνεται συσχετισμός μεταξύ νομικών κειμένων (σε ανθρώπινη γλώσσα) και του κώδικα των Έξυπνων Συμβολαίων.
- Η πλατφόρμα Corda σχεδιάστηκε για λειτουργία σύμφωνη με βιομηχανικά και επιχειρηματικά πρότυπα.
- Στην πλατφόρμα Corda, δεν υπάρχει έμφυτο κρυπτονόμισμα.

Η πλατφόρμα Corda αναπτύχθηκε από την εταιρεία R3 (R3CEV LLC). Η R3 είναι μια εταιρεία τεχνολογίας που ηγείται της προσπάθειας μιας κοινοπραξίας με περισσότερους από 80 από τους μεγαλύτερους χρηματοπιστωτικούς οργανισμούς παγκοσμίως. Σκοπός του εγχειρήματος είναι η έρευνα και ανάπτυξη γύρω από την εφαρμογή της τεχνολογίας Blockchain στον χρηματοπιστωτικό τομέα.

Ενδεικτικά παραθέτουμε ακολούθως ορισμένα από τα μέλη της κοινοπραξίας όπως Bank of America, Citi, Deutsche Bank, HSBC, Mitsubishi UFJ Financial Group, BNP Paribas, Toyota Financial Services, MetLife, Wells Fargo, UniCredit κ.α. Αποδεικνύεται συνεπώς πως στο εγχείρημα συμμετέχουν ορισμένοι από τους μεγαλύτερους χρηματοπιστωτικούς οργανισμούς παγκοσμίως.

Εικόνα 12: R3 CORDA Consortium (*https://www.corda.net/*)

ΚΕΦΑΛΑΙΟ 5: ΣΥΓΚΡΙΣΗ ETHEREUM, HYPERLEDGER FABRIC ΚΑΙ R3 CORDA

5.1 Σύγκριση Ethereum, Hyperledger Fabric και Corda

Στην παρούσα ενότητα, παρέχεται στον αναγνώστη μια σύντομη ανάλυση των βασικών διαφορών σε επίπεδο τεχνολογίας, ανάμεσα στις πλατφόρμες Κατανεμημένου Καθολικού (Distributed Ledger technologies [DLTs]) Ethereum, Hyperledger Fabric και Corda.

Ήδη από την εξέταση των Λευκών Βίβλων των Hyperledger Fabric, R3 Corda (αναφέρονται στη συνέχεια ως Fabric και Corda, αντίστοιχα) και Ethereum, είναι φανερό πως οι τρεις αυτές πλατφόρμες εξυπηρετούν διαφορετικούς σκοπούς, σε συνάρτηση με τα πιθανά πεδία εφαρμογής του κάθε πλαισίου. Τόσο το Fabric όσο και το Corda έχουν αναπτυχθεί για να εξυπηρετούν συγκεκριμένους σκοπούς, με τη διαφορά πως το Corda στοχεύει κυρίως σε εφαρμογές του χρηματοπιστωτικού τομέα. Αντίθετα, το Fabric έχει σκοπό την παροχή μιας βαθμωτής και επεκτάσιμης αρχιτεκτονικής με πιθανές εφαρμογές σε διάφορους κλάδους, από τον τραπεζικό κλάδο και τον κλάδο υγείας μέχρι και την εφοδιαστική αλυσίδα. Τέλος, η ομάδα του Ethereum παρουσιάζει την εν λόγω πλατφόρμα ως μη συσχετισμένη με κάποιο συγκεκριμένο πεδίο εφαρμογής. Ωστόσο, σε αντίθεση με το Fabric, το Ethereum δεν χαρακτηρίζεται από μια βαθμωτή αρχιτεκτονική, αλλά από την παροχή μιας γενικής πλατφόρμας, ικανής να υποστηρίξει κάθε είδους συναλλαγές και εφαρμογές.

Στον πίνακα που ακολουθεί, παρατίθενται συγκριτικά στοιχεία για τις τρεις πλατφόρμες που εξετάζουμε:

Characteristic	Ethereum	Hyperledger Fabric	R3 Corda
Description of platform	– Generic blockchain platform	– Modular blockchain platform	– Specialized distributed ledger platform for financial industry
Governance	– Ethereum developers	– Linux Foundation	– R3
Mode of operation	– Permissionless, public or private[4]	– Permissioned, private	– Permissioned, private
Consensus	– Mining based on proof-of-work (PoW) – Ledger level	– Broad understanding of consensus that allows multiple approaches – Transaction level	– Specific understanding of consensus (i.e., notary nodes) – Transaction level
Smart contracts	– Smart contract code (e.g., Solidity)	– Smart contract code (e.g., Go, Java)	– Smart contract code (e.g., Kotlin, Java) – Smart legal contract (legal prose)
Currency	– Ether – Tokens via smart contract	– None – Currency and tokens via chaincode	– None

Εικόνα 13: Ethereum VS Farbic VS Corda (Martin Valenta, Philipp Sandner, 2017)

Στη συνέχεια, εξετάζουμε αναλυτικά τα βασικά σημεία διαφοράς μεταξύ των τριών οικοσυστημάτων, πέραν των πιθανών πεδίων εφαρμογής της κάθε πλατφόρμας όπως αναλύθηκαν προηγουμένως.

5.1.1 Επίπεδο συμμετοχής των κόμβων του δικτύου στον μηχανισμό κοινής συναίνεσης (consensus)

Όσον αφορά το επίπεδο συμμετοχής των κόμβων του δικτύου στον μηχανισμό κοινής συναίνεσης κάθε πλατφόρμας, υπάρχουν ουσιαστικά δύο τρόποι λειτουργίας: σύστημα άνευ εξουσιοδότησης και σύστημα με εξουσιοδότηση (permissionless και permissioned συστήματα).

Σε ένα σύστημα άνευ εξουσιοδότησης, οι χρήστες που ελέγχουν κόμβους του δικτύου είναι είτε ανώνυμοι, είτε χρησιμοποιούν ψευδώνυμα. Το μοντέλο άνευ εξουσιοδότησης είναι αυτό με το οποίο το κοινό είναι περισσότερο εξοικειωμένο, αφού τα περισσότερο γνωστά Blockchain projects που είναι το Bitcoin και το Ethereum βασίζονται σε αυτό - με την έννοια ότι ο καθένας μπορεί να δημιουργήσει μια διεύθυνση και να αρχίσει να αλληλεπιδρά με το δίκτυο.

Αντίθετα, ένα σύστημα με εξουσιοδότηση είναι ένα κλειστό και υπό παρακολούθηση οικοσύστημα, όπου η πρόσβαση κάθε μέρους είναι πλήρως καθορισμένη και διαφορετική, ανάλογα με τον ρόλο κάθε χρήστη μέσα σε αυτό. Ένα σύστημα με εξουσιοδότηση δημιουργείται για να εξυπηρετεί ένα συγκεκριμένο σκοπό, με πλήρως ορισμένους κανόνες για τις συναλλαγές – που συνήθως ευθυγραμμίζονται με τις ανάγκες ενός συγκεκριμένου οργανισμού, ή μιας κοινοπραξίας εταιριών. Στην περίπτωση αυτή, οι χρήστες που θα συμμετέχουν στο οικοσύστημα είναι προκαθορισμένοι και η πρόσβαση στο δίκτυο επιτρέπεται μόνο σε αυτούς, όπως ισχύει και για τα Fabric και Corda.

5.1.2 Μηχανισμός κοινής συναίνεσης (consensus)

Ethereum.

Στην πλατφόρμα του Ethereum, το σύνολο των κόμβων που συμμετέχουν στο δίκτυο πρέπει απαραίτητα να συμφωνούν ως προς την λογική σειρά όλων των συναλλαγών που έχουν πραγματοποιηθεί εντός του οικοσυστήματος, άσχετα με το ένας κόμβος συμμετείχε σε κάποια από τις συναλλαγές ή όχι. Στην παρούσα έκδοση του Ethereum, ο μηχανισμός κοινής συναίνεσης επιτυγχάνεται μέσω της διαδικασίας εξόρυξης (mining), σύμφωνα με το μοντέλο proof-of-work (PoW). Όλοι οι κόμβοι του δικτύου πρέπει να συμφωνούν ως προς τη δομή και τα περιεχόμενα του Κατανεμημένου

Καθολικού, ενώ όλοι οι συμμετέχοντες έχουν πρόσβαση σε κάθε εγγραφή που έχει ποτέ πραγματοποιηθεί σε αυτό.

Λόγω του μοντέλου proof-of-work (PoW) που ακολουθείται στο Ethereum, η ταχύτητα επιβεβαίωσης των συναλλαγών εντός της πλατφόρμας επηρεάζεται αρνητικά. Ακόμη και όσον αφορά τα δεδομένα που περιέχονται στο καθολικό, ενώ οι εγγραφές είναι ανώνυμες, αυτές παραμένουν προσβάσιμες από όλους τους συμμετέχοντες, γεγονός που καθίσταται προβληματικό για εφαρμογές που απαιτούν μεγαλύτερο βαθμό ιδιωτικότητας.

Αντίθετα και όσον αφορά τα Fabric και Corda, επιτυγχάνεται αύξηση της ταχύτητας επιβεβαίωσης των συναλλαγών εντός του οικοσυστήματος, αφού μόνο τα μέρη που συμμετέχουν σε κάποια συναλλαγή αρκεί να συμφωνούν, για την επιβεβαίωσή της. Επιπροσθέτως και λόγω του μοντέλου με εξουσιοδότηση στο οποίο βασίζονται, παρέχουν δυνατότητες ελέγχου πρόσβασης στα περιεχόμενα του καθολικού και με αυτό τον τρόπο ενισχύεται η ιδιωτικότητα εντός του οικοσυστήματος.

Fabric.

Στην πλατφόρμα του Fabric, το μοντέλο κοινής συναίνεσης σχετίζεται με τη ροή της συναλλαγής, από την πρόταση για μια συναλλαγή στο δίκτυο από κάποιον χρήστη μέχρι και την καταγραφή της στο καθολικό. Επιπροσθέτως, οι κόμβοι του δικτύου αναλαμβάνουν διαφορετικούς ρόλους και εργασίες όσον αφορά τον μηχανισμό κοινής συναίνεσης, σε αντίθεση με το Ethereum, όπου όλοι οι κόμβοι του δικτύου συμμετέχουν εξίσου στη διαδικασία.

Στο οικοσύστημα του Fabric, οι κόμβοι του δικτύου διαφοροποιούνται ανάλογα με το αν είναι clients, peers or orderers. Ένας client λειτουργεί για λογαριασμό ενός χρήστη

και μπορεί να δημιουργεί και συνεπώς να επικαλείται συναλλαγές. Οι clients επικοινωνούν τόσο με τους peers, όσο και τους orderers. Οι peers είναι οι κόμβοι που διατηρούν τα δεδομένα του καθολικού και οι οποίοι λαμβάνουν μηνύματα από τους orderers για να καταγράψουν νέες συναλλαγές στο καθολικό. Στο σημείο αυτό αξίζει να αναφερθεί το γεγονός πως υφίσταται και ένα επιπλέον είδος κόμβου στο οικοσύστημα, που ονομάζεται endorser και σκοπός του είναι να εγκρίνει μια συναλλαγή, αφού έχει ελεγχθεί η εκπλήρωση συγκεκριμένων κριτηρίων, όπως η ύπαρξη των απαραίτητων υπογραφών. Τέλος, οι κόμβοι τύπου orderer παρέχουν ένα κανάλι επικοινωνίας στους clients και τους peers, μέσω του οποίου τα μηνύματα που σχετίζονται με τις συναλλαγές μπορούν να αποσταλούν. Όσον αφορά συγκεκριμένα τον μηχανισμό κοινής συναίνεσης, όλοι οι συνδεδεμένοι κόμβοι τύπου peers λαμβάνουν ακριβώς τα ίδια μηνύματα, με την ίδια ακριβώς λογική σειρά.

Ένα πρόβλημα που μπορεί να προκύψει από την όλη διαδικασία είναι η περίπτωση σφαλμάτων στην μεταφορά των μηνυμάτων, όταν δεν υπάρχει εμπιστοσύνη μεταξύ πολλών κόμβων τύπου Orderer εντός του δικτύου. Άμεση συνέπεια του προβλήματος είναι η ανάγκη ύπαρξης ενός αλγορίθμου κοινής συναίνεσης, ο οποίος θα χρησιμοποιείται για να έρθουν σε συμφωνία οι κόμβοι ασχέτως σφαλμάτων, όπως για παράδειγμα φαινόμενα ασυνέχειας στην λογική σειρά των μηνυμάτων, καθιστώντας με αυτόν τον τρόπο ανθεκτική σε σφάλματα την ανάπτυξη του Κατανεμημένου Καθολικού. Στο οικοσύστημα του Fabric, ο αλγόριθμος που χρησιμοποιείται επιλέγεται κατά περίπτωση, ανάλογα με τις συγκεκριμένες απαιτήσεις κάθε εφαρμογής.

Συμπερασματικά, είναι φανερό πως το Fabric χαρακτηρίζεται από επιλογές ως προς τον μηχανισμό κοινής συναίνεσης που θα χρησιμοποιηθεί σε κάθε εφαρμογή και επίσης από τη δυνατότητα ελέγχου πρόσβασης των κόμβων στις συναλλαγές,

αυξάνοντας με αυτόν το τρόπο την ταχύτητα επιβεβαίωσης των συναλλαγών και ενισχύοντας παράλληλα την ιδιωτικότητα εντός του οικοσυστήματος.

Corda.

Στην πλατφόρμα του Corda, όπως και στην περίπτωση του Fabric, για την επιβεβαίωση μιας συναλλαγής απαιτείται συμφωνία μόνο των κόμβων που συμμετέχουν σε αυτή. Απαιτείται κοινή συναίνεση τόσο για την ισχύ (validity) κάθε συναλλαγής, όσο και για τη μοναδικότητα (uniqueness) αυτής. Η ισχύς μιας συναλλαγής επιβεβαιώνεται μέσω της εκτέλεσης του κώδικα του έξυπνου συμβολαίου που σχετίζεται με αυτή και μέσω της επιβεβαίωσης της ύπαρξης όλων των απαραίτητων υπογραφών, καθώς και αφού ελεγχθεί πως οι συναλλαγές με τις οποίες σχετίζεται το έξυπνο συμβόλαιο είναι επίσης έγκυρες. Η μοναδικότητα αφορά τα states που μια συναλλαγή λαμβάνει ως είσοδο (input). Στο σημείο αυτό αξίζει να αναφερθεί πως state ονομάζεται κάθε αμετάβλητο στοιχείο της βάσης δεδομένων που αναπαριστά ένα γεγονός που είναι γνωστό σε έναν ή περισσότερους κόμβους του δικτύου σε μια συγκεκριμένη χρονική στιγμή. Συγκεκριμένα και όσον αφορά τη μοναδικότητα, πρέπει να επιβεβαιωθεί πως η υπό εξέταση συναλλαγή είναι ο μοναδικός καταναλωτής των states που δέχεται σαν είσοδο. Δηλαδή με άλλα λόγια, πρέπει να επιβεβαιωθεί πως δεν υπάρχει καμία άλλη συναλλαγή εντός του οικοσυστήματος που να καταναλώνει τα ίδια states. Και στην πλατφόρμα Corda, όπως και στο Fabric, ο αλγόριθμος κοινής συναίνεσης που χρησιμοποιείται επιλέγεται κατά περίπτωση, ανάλογα με τις συγκεκριμένες απαιτήσεις κάθε εφαρμογής.

5.1.3 Έξυπνα Συμβόλαια (Smart Contracts)

Ο κώδικας ενός Έξυπνου Συμβολαίου αποτελεί ουσιαστικά ένα λογισμικό γραμμένο σε κάποια προγραμματιστική γλώσσα. Στην πλατφόρμα του Fabric ο κώδικας Έξυπνων Συμβολαίων μπορεί να είναι γραμμένος σε γλώσσα Go ή Java, στο Ethereum σε γλώσσα Solidity και σε Java ή Kotlin στην περίπτωση του Corda. Όπως έχει προαναφερθεί, η πλατφόρμα του Ethereum είναι που αρχικά εισήγαγε την έννοια των Έξυπνων Συμβολαίων. Παράλληλα στο Fabric, ο όρος "chaincode" χρησιμοποιείται σαν ένα συνώνυμο των Έξυπνων Συμβολαίων. Επίσης, υπενθυμίζουμε στον αναγνώστη την χρήση κώδικα Έξυπνων Συμβολαίων για την επιβεβαίωση της ισχύος των συναλλαγών, στην πλατφόρμα του Corda.

Στο σημείο αυτό, γίνεται φανερό πως και οι τρεις πλατφόρμες που εξετάζουμε ενσωματώνουν τα Έξυπνα Συμβόλαια στη λειτουργία τους. Ωστόσο, υπάρχει μια σημαντική διαφορά ανάμεσα στα Fabric και Ethereum από τη μία και Corda από την άλλη. Στην πλατφόρμα του Corda, τα Έξυπνα Συμβόλαια δεν αποτελούνται μόνο από κώδικα, αλλά επιπροσθέτως μπορούν να περιέχουν και αποσπάσματα από νομικά κείμενα (σε ανθρώπινη γλώσσα). Στις πλατφόρμες των Fabric και Ethereum δεν υπάρχει αντίστοιχη δυνατότητα.

5.1.4 Έμφυτο κρυπτονόμισμα

Μια ακόμη διαφορά που χαρακτηρίζει τις υπό εξέταση πλατφόρμες είναι πως στο Ethereum, υπάρχει το έμφυτο κρυπτονόμισμα που ονομάζεται Ether (ETH). Οι μονάδες ETH χρησιμοποιούνται τόσο ως αμοιβές για τους κόμβους που συμμετέχουν στη διαδικασία εξόρυξης των μπλοκ, όσο και σαν τέλη για την πραγματοποίηση συναλλαγών, όπως έχει προαναφερθεί στην αντίστοιχη ενότητα. Συνεπώς, στο Ethereum είναι δυνατή η υλοποίηση dApps που να επιτρέπουν την μεταφορά αξίας

μεταξύ χρηστών. Επιπροσθέτως, ειδικές μονάδες κρυπτονομισμάτων μπορούν να δημιουργηθούν στα πλαίσια συγκεκριμένων εφαρμογών, μέσω της ανάπτυξης Έξυπνων Συμβολαίων που να συμμορφώνονται με συγκεκριμένες προδιαγραφές.

Στις πλατφόρμες Fabric και Corda δεν υπάρχει κάποιο έμφυτο κρυπτονόμισμα, αφού άλλωστε η κοινή συναίνεση (consensus) δεν επιτυγχάνεται μέσω της διαδικασίας εξόρυξης, όπως στο Ethereum. Ωστόσο στο Fabric, είναι δυνατή η δημιουργία ενός ψηφιακού νομίσματος μέσω chaincode. Αντίθετα στο Corda, δεν είναι εφικτή η δημιουργία κάποιου κρυπτονομίσματος.

5.2 Συμπεράσματα σύγκρισης

Αρχικά και όσον αφορά το Ethereum, ο μηχανισμός Έξυπνων Συμβολαίων που το χαρακτηρίζει το καθιστά μια πλατφόρμα γενικής χρήσης, ικανή να υποστηρίξει κάθε είδος εφαρμογής. Ωστόσο, η λειτουργία χωρίς εξουσιοδότηση και το γεγονός ότι οι πληροφορίες που περιέχονται στο κατανεμημένο καθολικό είναι προσβάσιμες από όλους του κόμβους του δικτύου, επηρεάζουν αρνητικά την ταχύτητα επιβεβαίωσης των συναλλαγών εντός της πλατφόρμας και μειώνουν τον βαθμό ιδιωτικότητας που χαρακτηρίζει το Ethereum.

Αντίθετα, το Fabric χαρακτηρίζεται από λειτουργία με εξουσιοδότηση, παρέχει επιλογές ως προς τον μηχανισμό κοινής συναίνεσης που θα χρησιμοποιηθεί σε κάθε εφαρμογή και επίσης παρέχει τη δυνατότητα ελέγχου πρόσβασης των κόμβων στις συναλλαγές, αυξάνοντας με αυτόν το τρόπο την ταχύτητα επιβεβαίωσης των συναλλαγών και ενισχύοντας παράλληλα την ιδιωτικότητα εντός του οικοσυστήματος. Επιπροσθέτως, το Fabric παρέχει μια βαθμωτή αρχιτεκτονική που του επιτρέπει να βρίσκει εφαρμογή σε διάφορους τομείς.

Το Corda έχει σχεδιαστεί συγκεκριμένα για εφαρμογές του χρηματοπιστωτικού τομέα, γεγονός που εξηγεί την απλοποιημένη αρχιτεκτονική του σε σχέση με το Fabric. Ωστόσο, δεδομένου ότι υπάρχουν αναφορές για συζητήσεις μεταξύ της εταιρείας R3 και της ομάδας του Hyperledger για ενσωμάτωση του Corda κάτω από την ομπρέλα του Hyperledger project, το Corda μπορεί να θεωρηθεί λύση συμπληρωματική του Fabric και όχι ανταγωνιστική.

ΚΕΦΑΛΑΙΟ 6: Η ΕΞΕΛΙΞΗ ΤΩΝ BLOCKCHAINS ΚΑΙ Η ΥΙΟΘΕΤΗΣΗ ΤΗΣ ΝΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΑΠΟ ΤΟΝ ΤΡΑΠΕΖΙΚΟ ΤΟΜΕΑ

6.1 Blockchains και τραπεζικός τομέας

Η εξέλιξη της τεχνολογίας γύρω από τα Blockchains έχει οδηγήσει αρκετούς να θεωρούν τις σχετικές εφαρμογές τόσο επαναστατικές, όσο και το διαδίκτυο περίπου δύο δεκαετίες πριν. Εκπρόσωποι του επιχειρηματικού κόσμου, από τον Bill Gates της Microsoft μέχρι τον ιδρυτή του Virgin Group, Richard Branson, εξυμνούν τις δυνατότητες της νέας τεχνολογίας. Οι υποστηρικτές μάλιστα θεωρούν πως δεν υπάρχουν όρια όσον αφορά τις πιθανές εφαρμογές των DLTs (Distributed Ledger Technologies).

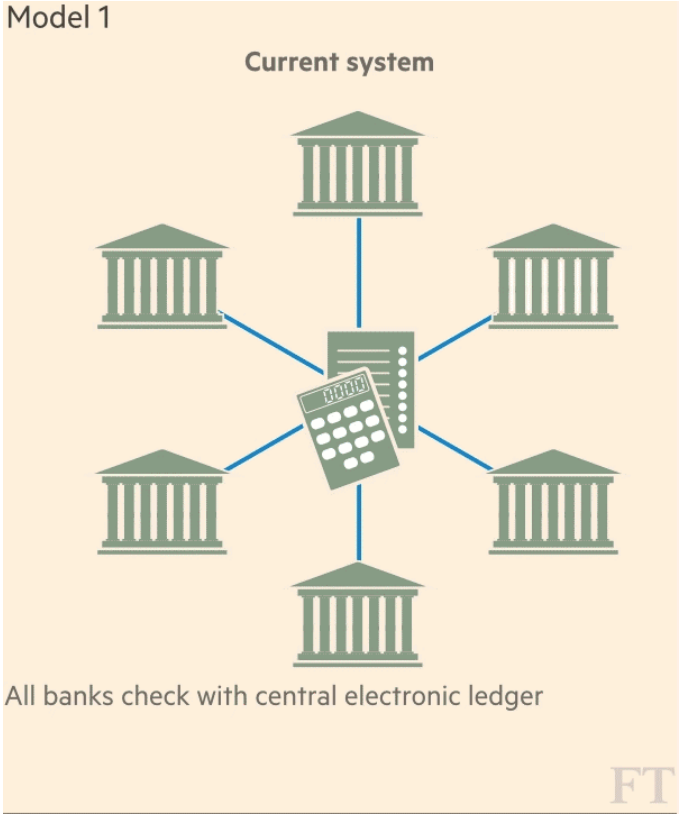
Τραπεζίτες, ασφαλιστές και εταιρείες όπως η IBM και η PWC ερευνούν τρόπους για να ενσωματώσουν την νέα τεχνολογία στη λειτουργία τους, η οποία στην απλούστερή της μορφή θα μπορούσε να ενώνει απευθείας τους καταναλωτές με τους προμηθευτές δημιουργώντας ειδικά δίκτυα, ελαχιστοποιώντας με αυτόν τον τρόπο την ανάγκη ύπαρξης μεσαζόντων στο μοντέλο.

Όσον αφορά συγκεκριμένα τον χρηματοπιστωτικό τομέα, η νέα τεχνολογία μπορεί να επισπεύσει πληθώρα διαδικασιών, μειώνοντας ιδιαίτερα τα σχετικά κόστη και αυξάνοντας εκθετικά την αποδοτικότητα, όπως θα αναλυθεί στη συνέχεια.

Στην παρούσα ενότητα επιχειρούμε να αναλύσουμε τον τρόπο με τον οποίο η εξέλιξη των DLTs καθιστά τη νέα τεχνολογία περισσότερο ελκυστική για τον τραπεζικό τομέα, εξετάζοντας 3 διαφορετικά μοντέλα:

1. **Το μοντέλο που ακολουθείται σήμερα στον τραπεζικό τομέα**

Στο μοντέλο που ακολουθείται σήμερα στον τραπεζικό τομέα, όλες οι πληροφορίες που αφορούν τις συναλλαγές που πραγματοποιούνται καταγράφονται σε ένα κεντρικό καθολικό, όπως φαίνεται και στην εικόνα 14:

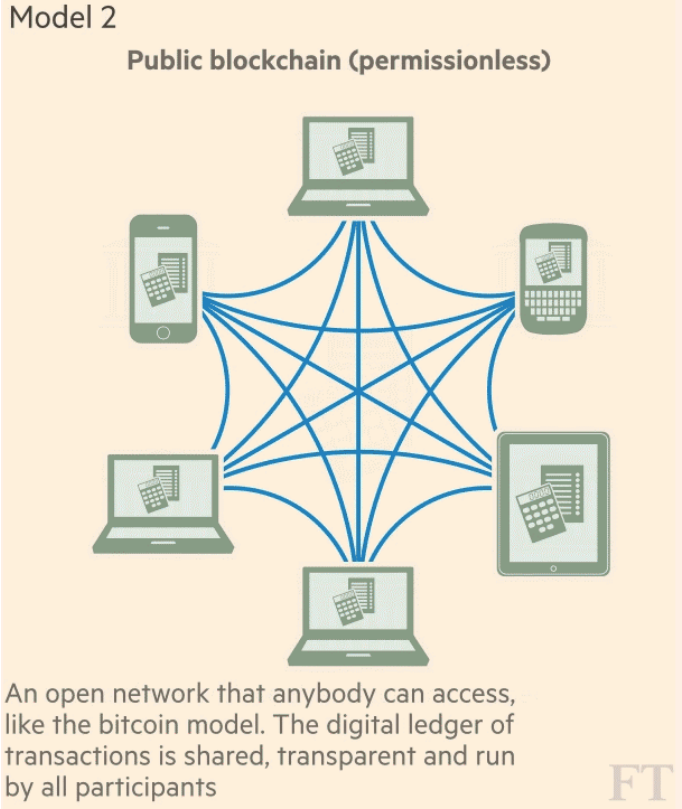


Εικόνα 14: Το μοντέλο που ακολουθείται σήμερα στον τραπεζικό τομέα (Jane Wild, Martin Arnold, Philip Stafford, 2015)

2. **Ένα μοντέλο λειτουργίας του τραπεζικού συστήματος βασισμένο σε ένα Permissionless Blockchain**

Σε ένα μοντέλο βασισμένο σε ένα Permissionless Blockchain - όπως το γνωστό σε όλους Bitcoin - υφίσταται ένα ανοιχτό δίκτυο στο οποίο καθένας μπορεί να έχει πρόσβαση. Όλοι οι κόμβοι του δικτύου πρέπει να συμφωνούν ως προς την εγκυρότητα μιας συναλλαγής, πριν αυτή καταγραφεί στο κατανεμημένο καθολικό.

Χρησιμοποιούνται κρυπτογραφικοί αλγόριθμοι για την ασφάλεια των δεδομένων και οι πληροφορίες που περιέχονται στο ψηφιακό καθολικό είναι διάφανες και προσβάσιμες από όλους, όπως φαίνεται και στην εικόνα 15:

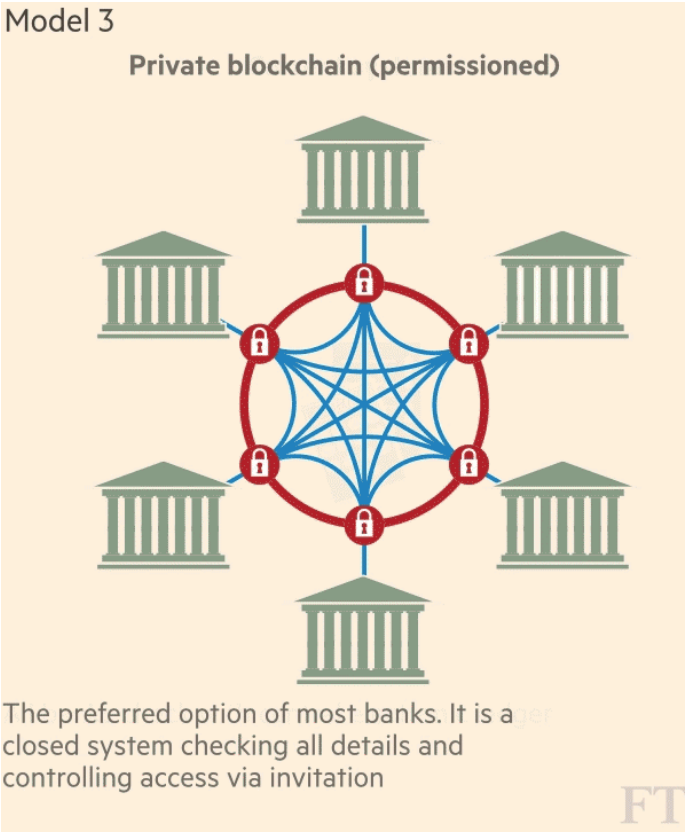


Εικόνα 15: Ένα μοντέλο λειτουργίας του τραπεζικού συστήματος βασισμένο σε ένα Permissionless Blockchain (Jane Wild, Martin Arnold, Philip Stafford, 2015)

3. Ένα μοντέλο λειτουργίας του τραπεζικού συστήματος βασισμένο σε ένα Permissioned Blockchain

Σε ένα μοντέλο λειτουργίας του τραπεζικού συστήματος βασισμένο σε ένα Permissioned Blockchain, υφίσταται ένα κλειστό και υπό παρακολούθηση οικοσύστημα, όπου η πρόσβαση κάθε μέρους είναι πλήρως καθορισμένη και διαφορετική, ανάλογα με τον ρόλο κάθε χρήστη μέσα σε αυτό. Υπάρχουν πλήρως

καθορισμένοι κανόνες για τις συναλλαγές που μπορούν να ευθυγραμμίζονται με τις ανάγκες ενός τραπεζικού οργανισμού, όπως φαίνεται και στην εικόνα 16:



Εικόνα 16: Ένα μοντέλο λειτουργίας του τραπεζικού συστήματος βασισμένο σε ένα Permissioned Blockchain (Jane Wild, Martin Arnold, Philip Stafford, 2015)

Παρατηρούμε συνεπώς, πως η εξέλιξη των Blockchains από τα Permissionless Blockchains στα Permissioned DLTs καθιστά τη νέα τεχνολογία περισσότερο ελκυστική για τον τραπεζικό τομέα. Αυτό συμβαίνει επειδή ένα μοντέλο βασισμένο σε ένα Permissioned Blockchain ενσωματώνει τα πλεονεκτήματα της νέας τεχνολογίας, όπως η πρόσβαση των ενδιαφερομένων μερών στις πληροφορίες που περιέχονται στο κατανεμημένο καθολικό σε πραγματικό χρόνο, ενώ παράλληλα παρέχει στην τράπεζες τον κεντρικό έλεγχο του συστήματος.

6.2 Εφαρμογές των Distributed Ledger Technologies [DLTs] στον τραπεζικό τομέα

Στην παρούσα ενότητα εξετάζουμε πέντε τρόπους με τους οποίους τα DLTs αναμένεται να επηρεάσουν την λειτουργία του τραπεζικού τομέα.

1. **Εκκαθαρίσεις και Διακανονισμοί**

Η συμβουλευτική εταιρεία Accenture έχει υπολογίσει ότι οι μεγάλες επενδυτικές τράπεζες θα μπορούσαν να εξοικονομήσουν 10.000.000$ εφαρμόζοντας την τεχνολογία Blockchain για να βελτιώσουν τις διαδικασίες που σχετίζονται με εκκαθαρίσεις και διακανονισμούς.

Ένα από τα περισσότερα γνωστά παραδείγματα αντίστοιχης εφαρμογής αποτελεί αυτό του οργανισμού Australian Securities Exchange, ο οποίος στοχεύει συσχετίσει τις διαδικασίες που ακολουθεί για εκκαθαρίσεις και διακανονισμούς με ένα σύστημα Blockchain.

Στις Ηνωμένες Πολιτείες Αμερικής, ο οργανισμός Depository Trust & Clearing Corporation [DTCC] συνεργάζεται με τις εταιρείες IBM, R3 και Axoni για να μεταφέρει τις πληροφορίες που σχετίζονται με συμβάσεις αντιστάθμισης πιστωτικού κινδύνου (Credit Default Swaps [CDS]) σε ένα σύστημα Blockchain. Εάν το εγχείρημα επιτύχει, η DTCC αναμένεται να ακολουθήσει την ίδια διαδικασία και για τις πληροφορίες που σχετίζονται με άλλα παράγωγα.

2. **Πληρωμές**

Οι κεντρικές τράπεζες παγκοσμίως ερευνούν τρόπους να εφαρμόσουν την τεχνολογία Blockchain στο σύστημα πληρωμών που ακολουθούν – ή ακόμη και να για εκδώσουν το δικό τους κρυπτονόμισμα. Σύμφωνα με την συμβουλευτική εταιρεία Accenture,

προς το παρόν οι κεντρικές τράπεζες απλά πειραματίζονται με τη νέα τεχνολογία, αφού η ανάπτυξη της νέας υποδομής για ένα σύστημα πληρωμών βασισμένο σε τεχνολογία Blockchain είναι μια ιδιαίτερα πολύπλοκη διαδικασία. Ένα επιπλέον πρόβλημα αποτελεί το γεγονός ότι το νέο σύστημα θα πρέπει να ενστερνιστούν αρκετές τράπεζες, για να έχει νόημα η εφαρμογή του.

Οι εμπορικές τράπεζες παράλληλα, που δεν μπορούν να περιμένουν τους κεντρικούς τραπεζίτες να οδηγήσουν τις εξελίξεις, πιέζουν προς την ίδια κατεύθυνση μέσω δικών τους projects. Η Ελβετική τράπεζα UBS έχει ανακοινώσει το "Utility Settlement Coin" project, σκοπεύοντας να δημιουργήσει ένα ψηφιακό νόμισμα κατάλληλο για χρήση στις χρηματοοικονομικές αγορές, αφού οι ψηφιακές μονάδες αξίας θα μετατρέπονται σε φυσικό συνάλλαγμα αφότου κατατεθούν στις κεντρικές τράπεζες.

3. Χρηματοδότηση επιχειρήσεων

Οι διαδικασίες που σχετίζονται με την χρηματοδότηση των επιχειρήσεων σήμερα βασίζονται στην αποστολή παραστατικών όπως εγγυητικές επιστολές σε φυσική (χάρτινη) μορφή (εφόσον συνήθως απαιτούνται σφραγίδες και υπογραφές για την επικύρωση ενός εγγράφου), μέσω ταχυδρομείου ή fax και πολλοί τραπεζίτες αναζητούν τον εκσυγχρονισμό του μοντέλου. Εφόσον στην συγκεκριμένη περίπτωση είναι απαραίτητο πολλά ενδιαφερόμενα μέρη να έχουν πρόσβαση στις ίδιες ακριβώς πληροφορίες, η τεχνολογία Blockchain φαίνεται να αποτελεί λύση του προβλήματος. Σύμφωνα με την Accenture, σε μια μεταφορά αγαθών από την Κίνα, ακόμη και πενήντα διαφορετικοί άνθρωποι χρειάζονται πρόσβαση στις σχετικές με την αποστολή πληροφορίες, την ίδια σχεδόν χρονική στιγμή.

4. Ταυτοποίηση

Η ταυτοποίηση των πελατών και των αντισυμβαλλόμενων μερών είναι κρίσιμης σημασίας για τον τραπεζικό τομέα. Οι τράπεζες προσπαθούν εδώ και χρόνια να εφαρμόσουν ένα ψηφιακό εργαλείο αποθήκευσης και διαμοιρασμού της ταυτότητας των πελατών τους. Μέχρι στιγμής το εγχείρημα έχει αποτύχει, αλλά πιστεύεται πως ένα σύστημα βασισμένο σε Blockchain θα μπορούσε να αποτελεί λύση. Τα αποθηκευμένα δεδομένα θα προστατεύονται μέσω κρυπτογραφίας και κάθε ενδιαφερόμενο μέρος θα έχει πρόσβαση στις πληροφορίες του κατανεμημένου καθολικού, σε πραγματικό χρόνο.

5. Κοινοπρακτικά δάνεια

Στις Ηνωμένες Πολιτείες Αμερικής, όταν μια εταιρεία λαμβάνει χρηματοδότηση μέσω κοινοπρακτικού δανείου, απαιτούνται κατά μέσον όρο 19 ημέρες για την διεκπεραίωση όλων των σχετικών διαδικασιών από τις τράπεζες. Όταν ένα δάνειο μεταφέρεται από μια τράπεζα σε άλλη ή όταν ο δανειζόμενος ξεπληρώσει το δάνειο νωρίτερα από τον προβλεπόμενο χρόνο, η αποστολή των σχετικών εγγράφων μεταξύ των τραπεζών συνήθως πραγματοποιείται μέσω fax.

Η Credit Suisse είναι ένας από τους 19 χρηματοπιστωτικούς οργανισμούς που έχουν σχηματίσει κοινοπραξία και συνεργάζονται με την εταιρεία Synaps, για να μεταφέρουν τις πληροφορίες που σχετίζονται με κοινοπρακτικά δάνεια σε ένα σύστημα Blockchain.

ΚΕΦΑΛΑΙΟ 7: ΕΦΑΡΜΟΓΕΣ ΤΩΝ BLOCKCHAINS

7.1 Digital Trade Chain

Τον Ιούνιο του 2017 η IBM ανακοίνωσε πως έχει αναλάβει την ανάπτυξη εφαρμογής τεχνολογίας Blockchain, που θα χρησιμοποιηθεί από επτά από τις μεγαλύτερες τράπεζες της Ευρώπης ώστε να διευκολύνει το διεθνές εμπόριο για μικρές και μικρομεσαίες επιχειρήσεις.

Η υπό σχεδίαση λύση ονομάζεται Digital Trade Chain (Ψηφιακή Αλυσίδα Εμπορίου) και θα βασίζεται στην πλατφόρμα του Hyperledger Fabric. Σκοπός της εφαρμογής είναι να φέρει σε επαφή τα συμβαλλόμενα μέρη που επιθυμούν να εκτελέσουν κάποια εμπορική συναλλαγή, μέσω της τεχνολογίας Blockchain. Το δίκτυο των τραπεζών θα αποτελεί την βάση εμπιστοσύνης των συναλλασσομένων, αφού θα είναι υπεύθυνο για την τελική μεταφορά των χρημάτων που θα σημαίνει και την ολοκλήρωση της διαδικασίας συναλλαγής, ενώ η διαχείριση της διαδικασίας θα υλοποιείται αποκλειστικά μέσω της τεχνολογίας Blockchain.

Το έργο αποτελεί ουσιαστικά την πρώτη εφαρμογή της τεχνολογίας Blockchain σε τραπεζικούς οργανισμούς.

Το Digital Trade Chain Consortium είναι μια κοινοπραξία των τραπεζών Deutsche Bank, HSBC, KBC, Natixis, Rabobank, Societe Generale and Unicredit.

7.2 Εφαρμογές Blockchain σύμφωνα με το World Economic Forum

Το World Economic Forum τον Δεκέμβρη του 2016 δημοσίευσε άρθρο σχετικά με τέσσερις πιθανές μελλοντικές εφαρμογές της τεχνολογίας BC, αναγνωρίζοντας πως:

- Το ένα πέμπτο του παγκόσμιου πληθυσμού – προσεγγιστικά 1.5 δισεκατομμύριο άνθρωποι – δεν έχουν στην κατοχή τους κάποιο επίσημο έγγραφο που να αποδεικνύει την ταυτότητά τους. Σύμφωνα με την παγκόσμια τράπεζα, οι περισσότεροι ζουν στην Ασία και την Αφρική και στην συντριπτική τους πλειοψηφία είναι γυναίκες και παιδιά. Χωρίς επίσημα έγγραφα, οι άνθρωποι αυτοί είναι «αόρατοι» στο κοινωνικό μας σύστημα και το γεγονός αυτό τους καθιστά ευάλωτους στο δουλεμπόριο, την πορνεία και την εκμετάλλευση. Η Microsoft έχει ανακοινώσει την ανάπτυξη συστήματος secure identity βασισμένο στην τεχνολογία Blockchain, ώστε να είναι δυνατή η ανεξάρτητη ταυτοποίηση πολιτών.
- Το Kimberley Process, η διεθνής επιτροπή για την μείωση του εμπορίου διαμαντιών σε εμπόλεμες περιοχές που συστάθηκε το 2003, ερευνά τρόπους χρήσης της τεχνολογίας Blockchain που να επιτρέπουν την ιχνηλασιμότητα των διαμαντιών. Η νεοφυής επιχείρηση Everledger ήδη χρησιμοποιεί το Blockchain για να βεβαιώσει ψηφιακά την ιδιοκτησία διαμαντιών. Αντίστοιχη εφαρμογή θα μπορούσε να χρησιμοποιηθεί και για την καταπολέμηση τους λαθρεμπορίου ελεφαντοστού, ενώ στο χώρο της μόδας ήδη γίνονται προσπάθειες χρήσης του Blockchain ενάντια στο εμπόριο πλαστών προϊόντων.
- Στο χώρο της μουσικής βιομηχανίας, το Blockchain αντιμετωπίζεται ως ένας τρόπος να έρθουν οι καλλιτέχνες σε άμεση επαφή με τους μουσικόφιλους πουλώντας τη μουσική τους απευθείας στο κοινό, εξαλείφοντας με αυτό τον τρόπο την ανάγκη για μεσάζοντες. Η βραβευμένη με Grammy συνθέτης και τραγουδιστής Imogen Heap κυκλοφόρησε το τραγούδι Tiny Human χρησιμοποιώντας πλατφόρμα Blockchain, όπου οι χρήστες πληρώνουν την

πρόσβαση στο τραγούδι και το αντίτιμο διαμοιράζεται αυτόματα ανάμεσα στους μουσικούς.

- Η Σουηδία πειραματίζεται σχετικά με την ανάπτυξη συστήματος καταγραφής τίτλων ιδιοκτησίας γης βασισμένο σε Blockchain. Στόχος είναι μέσω της τεχνολογίας οι όροι κάθε συναλλαγής σχετικής με αγοραπωλησία ακινήτων να καταγράφονται στο Blockchain και όλες οι ομάδες εμπλεκομένων όπως τράπεζες, μεσίτες, κυβερνήσεις, αγοραστές και πωλητές να έχουνε ελεύθερη πρόσβαση σε αυτούς. Ειδικά στον αναπτυσσόμενο κόσμο θα μπορούσε με αυτόν τον τρόπο να καταπολεμηθεί η διαφθορά, να μειωθεί το ποσοστό της αδήλωτης γης και επίσης να ενισχυθεί το ποσοστό δανείων για αγορά γης ή κατοικίας που οι τράπεζες δύνανται να εγκρίνουν. Στις Ονδούρες, μία από τις φτωχότερες χώρες της Αμερικής, η κυβέρνηση είναι σε συζητήσεις για την ανάπτυξη κατανεμημένης βάσης δεδομένων με τίτλους ιδιοκτησίας, ενώ αντίστοιχες προσπάθειες γίνονται και στην Γκάνα, όπου υπολογίζεται πως το 78% της γης είναι αδήλωτη.

7.3 Blockchains και η βιομηχανία φαρμάκων

Η βιομηχανία φαρμάκων, στην προσπάθειά της να περιορίσει το μακροχρόνιο πρόβλημα της ροής κλεμμένων ή πλαστών φαρμάκων στην εφοδιαστική αλυσίδα και μέσω αυτής στους ασθενείς, στρέφεται στην τεχνολογία Blockchain. Τον Σεπτέμβρη του 2017, ομάδα εταιρειών ανακοίνωσε το MediLedger project, το οποίο χρησιμοποιεί εφαρμογές Blockchain για να διαχειριστεί την εφοδιαστική αλυσίδα φαρμάκων. Η κοινοπραξία, που περιλαμβάνει γίγαντες της βιομηχανίας φαρμάκων όπως η Genetech και η Pfizer, έχει ήδη ολοκληρώσει επιτυχώς πιλοτική εφαρμογή που της επιτρέπει την ιχνηλασιμότητα των φαρμάκων.

Εάν το εγχείρημα επιτύχει, όλα τα μέρη της εφοδιαστικής αλυσίδας – από τον παραγωγό έως τους χονδρέμπορους και τα νοσοκομεία – θα καταγράφουν όλες τις παραλαβές φαρμάκων στο Κατανεμημένο Καθολικό. Πρακτικά, σε κάθε βήμα της διαδικασίας διανομής, ένα δίκτυο υπολογιστών θα εγγυάται την προέλευση και την αυθεντικότητα ενός φορτίου φαρμάκων – αποτρέποντας με αυτό τον τρόπο τις ληστείες καθώς και την πλαστογράφηση φαρμάκων. Επίσης, το εγχείρημα θα εισάγει ταχύτητα στην όλη διαδικασία, αφού σε περίπτωση που κάποιο φορτίο χαθεί, τα δεδομένα που περιέχονται στο κατανεμημένο καθολικό θα επιτρέπουν σε όλα τα συμμετέχοντα μέρη να εντοπίσουν το φορτίο καθώς και την εταιρία που το είχε τελευταία στην κατοχή της.

Σύμφωνα με τον Ryan Orr Της Chronicled, της εταιρίας με έδρα το Σαν Φρανσίσκο που έχει αναλάβει την ανάπτυξη των εφαρμογών Blockchain του MediLedger, η βιομηχανία φαρμάκων ήδη χρησιμοποιεί εξειδικευμένα λογισμικά για την διαχείριση της διανομής φαρμάκων, τα οποία τελικά σχηματίζουν ένα ασύνδετο δίκτυο Βάσεων Δεδομένων. Σύμφωνα με τον Ryan Orr, η εισαγωγή ενός συστήματος Blockchain, στο οποίο κάθε συμμετέχων ελέγχει έναν κόμβο του δικτύου και όπου κάθε συναλλαγή επιβεβαιώνεται μόνο με συμφωνία των κόμβων (consensus) είναι σίγουρα ένα βήμα μπροστά.

Στο σημείο αυτό αξίζει να σημειωθεί πως οι βιομηχανίες φαρμάκων δεν πρωτοτυπούν στην χρήση BC για την καλύτερη διαχείριση των γραμμών διανομής. Η βιομηχανία διαμαντιών συνεργάζεται με την εταιρία Everledger για να επιβεβαιώσει την προέλευση πολύτιμων λίθων *(ήδη έχουν εγγραφεί πάνω από 1.6 εκατομμύρια λίθοι στο κατανεμημένο καθολικό),* ενώ στο εμπόριο τροφίμων - με πρωτεργάτη την Walmart – το Blockchain χρησιμοποιείται για την ιχνηλασιμότητα χοιρινού κρέατος και πουλερικών. Παράλληλα, η πολιτεία Delaware των Ηνωμένων Πολιτειών έχει

υπερψηφίσει νόμο, που επιτρέπει σε εταιρίες να δημοσιεύουν την μετοχική τους δομή και άλλα εταιρικά αρχεία σε Blockchain.

Το MediLedger Project, που υποστηρίζεται από την Συμβουλευτική σε θέματα εφοδιαστικής αλυσίδας The LinkLab, αναπτύσσει το λογισμικό της χρησιμοποιώντας το Quorum – την έκδοση του πρωτοκόλλου Ethereum για επιχειρήσεις που υποστηρίζεται από την J.P. Morgan.

7.4 Πιλοτικό πρόγραμμα Blockchain από το Υπουργείο Υγείας της Ρωσίας

Το Υπουργείο Υγείας της Ρωσίας συνεργάζεται με μία από τις μεγαλύτερες Κρατικές Τράπεζες της χώρας, την Vnesheconombank (VEB), για την διερεύνηση πιθανών εφαρμογών της τεχνολογίας Blockchain. Συγκεκριμένα ερευνούνται μέθοδοι για την ανταλλαγή ιστορικών δεδομένων για τους ασθενείς στο σύστημα Υγείας, ενώ συγχρόνως γίνονται προσπάθειες για την ανάπτυξη συστήματος ανταλλαγής δεδομένων μεταξύ διαφόρων κρατικών υπηρεσιών.

Η τράπεζα αποκάλυψε επίσης πως θα ιδρύσει ένα «Κέντρο Δεξιοτήτων» μέσω του οποίου θα διερευνηθούν οι πιθανές εφαρμογές των τεχνολογιών Blockchain, ενώ κάλεσε και την κυβέρνηση να συμμετάσχει σε αυτήν τη ομάδα εργασίας. Ο Sergey Gorkov, πρόεδρος της τράπεζας, δήλωσε πως γίνονται προσπάθειες για την ανάπτυξη προϊόντων και υπηρεσιών γύρω από την νέα αυτή τεχνολογία, οι οποίες κυρίως επικεντρώνονται γύρω από τομείς της Διαχείρισης Έργων και της εφοδιαστικής αλυσίδας, ενώ σχετικές αναφορές θέλουν την τράπεζα να ερευνά επίσης μεθόδους συγκέντρωσης κεφαλαίων για φιλανθρωπίες βασισμένους στην πλατφόρμα του Ethereum.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Michael Crosby, Nachiappan, Pradan Pattanayak, Snajeev Verma, Vignesh Kalyanaraman (2016) 'Blockchain Technology: Beyond Bitcoin' *Berkeley's Applied Innovation Review, Issue No.2, June 2016.*
2. Christian Cachin (2016) 'Blockchain – From the Anarchy of Cryptocurrencies to the Enterprise' *IBM Research.*
3. Wikipedia: 'Blockchain'
4. Investopedia: 'Blockchain'
5. Doug Sleeter (2017) 'The promise of Blockchain Technology' *Accountex Report*
6. Investopedia: 'Double-Spending'
7. John Kelleher (2017) 'What is Bitcoin Mining?' *Investopedia*
8. Ethereum: History of Ethereum *http://ethdocs.org/en/latest/introduction/history-of-ethereum.html*
9. Bits on Blocks (2016) 'A gentle introduction to Ethereum' *https://bitsonblocks.net/2016/10/02/a-gentle-introduction-to-ethereum/*
10. Wikipedia: 'Contract'
11. Βικιπαίδεια: 'Σύμβαση'
12. Nick Szabo (1996) 'Smart Contracts: Building Blocks for Digital Markets'
13. Aaron Wright, Primavera De Filippi (2015) 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia'
14. Alan Morrison (2016) 'How smart contracts automate digital business' *PWC: Next in Tech*
15. Nick Szabo (1999) 'A Formal Language for Analyzing Contracts'
16. Etherscripter.com: 'What is Ethereum'
17. Ethereum: Introduction to Smart Contracts *http://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html*
18. Ethereum White Paper *https://github.com/ethereum/wiki/wiki/White-Paper#applications*
19. Alyssa Hertig 'What is a Decentralized Application' *Coindesk*
20. Blockchainhub.net: Decentralizes Applications – dApps *https://blockchainhub.net/decentralized-applications-dapps/*
21. Robert Hackett, Anna Teregulova (2017) 'Why Everyone's Talking About 'Initial Coin Offerings'' *Fortune*
22. Blockgeeks.com: What is an Initial Coin Offering? Raising millions in seconds *https://blockgeeks.com/guides/what-is-an-initial-coin-offering/*
23. Wikipedia: 'Mastercoin'
24. Wikipedia: 'The DAO (organization)'
25. Bits on Blocks (2016) 'A gentle introduction to smart contracts' *https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/*
26. Don Tapscott, Alex Tapscott (2016) 'Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world' *Penguin Random House LLC*
27. Wikipedia: 'Hyperledger'

28. Hyperledger: *https://www.hyperledger.org/*
29. Wikipedia: 'R3 (company)'
30. R3: 'Corda Solution Guide' *https://www.corda.net/wp-content/uploads/2017/10/Corda-Solution-Guide.pdf*
31. R3: 'Introducing R3 Corda: A Distributed Ledger Designed for Financial Services' *http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services*
32. Martin Valenta, Philipp Sandner (2017) 'Comparison of Ethereum, Hyperledger Fabric and Corda' *Frankfurt School Blockchain Center*
33. Devon Allaby (2016) 'The trust trade-off: Permissioned VS permissionless blockchains' *Accenture*
34. Jane Wild, Martin Arnold, Philip Stafford (2015) 'Technology: Banks seek the key to blockchain' *Financial Times*
35. Martin Arnold (2017) 'Five ways banks are using blockchain' *Financial Times*
36. Arjun Kharpal (2017) 'Blockchain technology is moving into the financial mainstream with IBM and seven European banks' *CNBC*
37. IBM: 'Seven Major European Banks Select IBM to Bring Blockchain-Based Trade Finance to Small and Medium Enterprises' *http://www-03.ibm.com/press/us/en/pressrelease/52706.wss*
38. World Economic Forum: 'Beyond Bitcoin: 4 surprising uses for Blockchain' *https://www.weforum.org/agenda/2016/12/fighting-human-trafficking-tracing-blood-diamonds-and-other-surprising-uses-for-blockchain/*
39. Jeff John Roberts (2017) 'Big Pharma turns to Blockchain to track meds' *Fortune*
40. Stan Higgins (2017) 'Russia's Ministry of Health is launching a Blockchain pilot' *Coindesk*