Smart Contracts

Καθηγητές:

Σπυράντης Λύσσανδρος

Σπυράντης Θεόδωρος

Τα Smart contracts(έξυπνες συμβάσεις ή έξυπνα συμβόλαια) είναι προγράμματα τα οποία είναι αποθηκευμένα στο blockchain. Έχουν την ονομασία «συμβόλαια» επειδή προκειμένου να πραγματοποιειθεί το πρόγραμμα θα πρέπει πρώτα να εκπληρώνονται όλες οι προϋποθέσεις, ακριβώς όπως σε ένα συμβόλαιο.

Ένα από τα πιο σημαντικά χαρακτηριστικά που προσφέρει το blockchain είναι ότι, επειδή είναι ένα αποκεντρωμένο(decentralized) σύστημα που υπάρχει ανάμεσα σε όλους τους χρήστες, δεν υπάρχει κανένας λόγος να πληρώσετε μεσάζοντες (middlemen) και σας εξοικονομεί χρόνο και χρήματα. Τα blockchain έχουν τα προβλήματά τους, αλλά αναμφισβήτητα έχουν αξιολογηθεί γρηγορότερα, φθηνότερα και ασφαλέστερα από τα παραδοσιακά συστήματα, για αυτό και οι τράπεζες και οι κυβερνήσεις στρέφονται προς αυτά.

Το 1994, ο Nick Szabo, νομικός, ερευνητής και κρυπτογράφος, συνειδητοποίησε ότι το αποκεντρωμένο ledger(λογιστικό "βιβλίο") θα μπορούσε να χρησιμοποιηθεί για smart contracts , διαφορετικά αποκαλούμενες συμβάσεις αυτοελέγχου, αποκλειστικές συμβάσεις ή ψηφιακές συμβάσεις. Σε αυτή τη μορφή, οι συμβάσεις θα μπορούσαν να μετατραπούν σε κώδικα υπολογιστή, να αποθηκευτούν και να αναπαραχθούν στο σύστημα, και να επαληθεύονται από το δίκτυο υπολογιστών που τρέχουν το blockchain. Αυτό θα οδηγήσει επίσης σε feedback στο ledger, όπως η μεταφορά χρημάτων και η παραλαβή του προϊόντος ή της υπηρεσίας. (blockgeeks, 2016).

Τι είναι τα Smart Contracts;

Τα Smart Contracts τα οποία ονομάζονται επίσης distributed apps, δηλαδή κατανεμημένες εφαρμογές, βοηθούν στο να ανταλλάξετε χρήματα, ακίνητα, μετοχές ή οτιδήποτε είναι πολύτιμο με διαφανή τρόπο, χωρίς εμπόδια, αποφεύγοντας παράλληλα τις υπηρεσίες ενός μεσάζοντος.

Τα smart contracts είναι ακριβώς όπως τα συμβόλαια στον πραγματικό κόσμο, η μόνη διαφορά είναι ότι είναι εντελώς ψηφιακά.

Δεν συνδέονται κατ 'ανάγκη με την κλασσική έννοια της σύμβασης, αλλά μπορεί να αποτελούν οποιοδήποτε είδος προγράμματος ηλεκτρονικού υπολογιστή το οποίο αποθηκεύεται σε ένα blockchain.

Ο καλύτερος τρόπος για να περιγράψετε τα smart contracts είναι να συγκρίνετε την τεχνολογία τους με μια μηχανή αυτόματης πώλησης.

Συνήθως, θα πάτε σε δικηγόρο ή συμβολαιογράφο, θα τους πληρώσετε και θα περιμένετε έως ότου λάβετε το έγγραφο. Τα smart contracts, απλώς παίρνουν τα λεφτά που τους έχετε δώσει (π.χ. 1 bitcoin), και είστε έτοιμοι για την παραλαβή του προϊόντος ή της υπηρεσίας.

Παράδειγμα 1:

Για την κατανόηση των smart contracts ας υποθέσουμε ότι νοικιάσατε ένα διαμέρισμα από μένα. Μπορείτε να το κάνετε αυτό μέσω του blockchain πληρώνοντας με κρυπτονομίσματα. Παίρνετε μια απόδειξη η οποία αποθηκεύεται στο smart contract. Σας δίνω το ψηφιακό κλειδί εισόδου(digital entry key) το οποίο έρχεται σε εσάς μια προκαθορισμένη ημερομηνία. Αν το κλειδί δεν έχει έρθει την προκαθορισμένη ημερομηνία, το blockchain σας στέλνει μια επιστροφή χρημάτων. Αν στείλω το κλειδί πριν από την προκαθορισμένη ημερομηνία ενοικίασης, η λειτουργία του smart contract κρατά την αμοιβή μου καθώς και το κλειδί εσάς αντίστοιχα, έως ότου έρθει η προκαθορισμένη ημερομηνία. Το σύστημα λειτουργεί βάση της συνάρτησης If-Then, δηλαδή εάν εκπληρωθούν οι προηποθέσεις τότε θα "τρέξει" κανονικά και το συμβόλαιο. Και τέλος το συμβόλαιο θα επαλυθευτεί από εκατοντάδες ανθρώπους.

Έτσι εάν σας δώσω το κλειδί, είμαι σίγουρος ότι θα λάθω την ανταμοιβή μου. Αν στείλετε το προκαθορισμένο ποσό σε bitcoins, θα λάβετε το κλειδί. Το έγγραφο ακυρώνεται αυτόματα μετά την πάροδο του χρόνου και ο κώδικας δεν μπορεί να παρεμβληθεί από κανέναν από εμάς χωρίς να το γνωρίζει ο άλλος, καθώς όλοι οι συμμετέχοντες ενημερώνονται ταυτόχρονα.(Syed Jafar Naqvi, 2017).

Παράδειγμα 2:

Ένα ακόμα παράδειγμα χρήσης των smart contracts είναι τα ICO(initial coin offerings), στα οποία θα αναφερθούμε αργότερα για το πως ακριβώς δουλεύουν.

Όταν ξεκινάει ένα νέο decentralized project και θέλει να μοιράσει τα tokens(κρυπτονομίσματα) του μέσο ενός ICO χρησημοποιεί ένα smart contract. Για παράδειγμα ένα ICO στο blockchain του Ethereum θα πουλάει τα νομίσματα του νέου project έναντι Ethereum tokens με την χρήση ενός smart contract. Τα tokens αυτά θα πάνε στην ομάδα του project και η ομάδα με την σειρά της θα μοιράσει τα tokens της στους αγοραστές στην προκαθορισμένη τιμή.

Αυτό που συμβαίνει δηλαδή είναι, η ομάδα του project δημιουργεί ένα smart contract το οποίο μόλις πάρει τα Ethereum που χρειάζεται στέλνει τα αντίστοιχα tokens στους αγοραστές μέχρι να φτάσει το όριο των tokens που έχει να μοιράσει.

Φυσικά μπορεί να έχει επιπλέον περιορισμούς το smart contract όπως όριο επένδυσης ανά άτομο ή οτιδήποτε έχει ορίσει η συγκεκριμένη ομάδα.

Ποιο συγκεκριμένα, τα smart contracts όχι μόνο καθορίζουν τους κανόνες και τις κυρώσεις για μια συμφωνία με τον ίδιο τρόπο όπως μια παραδοσιακή σύμβαση, αλλά αυτομάτως επιβάλλουν αυτές τις υποχρεώσεις.

Μπορούμε να προγραμματίσουμε το smart contract έτσι ώστε να κρατάνε όλα τα εισπραχθέντα κεφάλαια μέχρι να επιτευχθεί ο στόχος.
Οι υποστηρικτές ενός έργου μπορούν πλέον να μεταφέρουν τα χρήματά τους στο smart contract.
Εάν το έργο χρηματοδοτηθεί πλήρως, το smart contract μεταβιβάζει αυτόματα τα χρήματα στον δημιουργό του έργου.
Και αν το έργο δεν ανταποκριθεί στον στόχο, τα χρήματα πηγαίνουν αυτόματα στους υποστηρικτές.

Με αυτή την τεχνική, κανείς δεν έχει τον έλεγχο των χρημάτων.
Αλλά γιατί πρέπει να εμπιστευόμαστε ένα smart contract;
Επειδή τα smart contracts αποθηκεύονται σε ένα blockchain, έχουν κληρονομήσει κάποιες ενδιαφέροντες ιδιότητες.

Μερικές από τις ιδιότητες τους είναι:

- Είναι **αυτόματα**
- Είναι **γρήγορα**
- Εκτελούνται **απευθείας**
- Είναι **φθηνά**
- Είναι **διαφανή** και **κατανεμημένα**
- Είναι **αμετάβλητα**

Ποιο επεξηγηματικά τα smart contracts κάνουν διαφορετικές διαδικασίες να εκτελούνται αυτόματα και δεν χρειάζεται να επιβλέπετε την εκπλήρωση της σύμβασης, τα μαθηματικά το κάνουν για σας.. Είναι γρήγορα αφού εκτελούνται μέσα σε λίγα δευτερόλεπτα καθώς δεν εμπλέκονται μεσάζοντες και η επαλήθευση έρχεται από το ίδιο το smart contract. Επίσης δεν πληρώνονται φόροι (fees) για την εκτέλεση τους.

Όταν λέμε ότι είναι αμετάβλητα σημαίνει ότι μόλις δημιουργηθεί ένα smart contract, δεν μπορεί ποτέ να αλλάξει ξανά. Έτσι, κανείς δεν μπορεί να πάει πίσω από την πλάτη σας και να παραβιάσει τον κώδικα της σύμβασής σας.
Ενώ όταν λέμε ότι είναι κατανεμημένα, σημαίνει ότι το αποτέλεσμα της σύμβασής σας επικυρώνεται από όλους στο δίκτυο(blockchain).
Έτσι, ένα άτομο δεν μπορεί να αναγκάσει το smart contract να απελευθερώσει τα χρήματα, επειδή άλλοι άνθρωποι στο δίκτυο θα εντοπίσουν αυτήν την προσπάθεια και θα την χαρακτηρίσουν ως άκυρη.

Για τους παραπάνω λόγους η παραβίαση των smart contracts καθίσταται σχεδόν αδύνατη. (Mayank Pratap, 2018).

Τα προβλήματα των Smart Contracts

Τα smart contracts όμως δεν είναι τέλεια. Τι γίνεται αν υπάρξουν bugs(σφάλματα) στον κώδικα; Ή πώς θα έπρεπε οι κυβερνήσεις να ρυθμίζουν τους νόμους για αυτές τις συμβάσεις; Ή πώς θα χρεώνουν οι κυβερνήσεις αυτές τις συναλλαγές;

Θα χρησιμοποιήσουμε ως παράδειγμα την κατάσταση ενοικίασής ενός διαμερίσματος από πριν.

Τι γίνεται αν υπάρξει λάθος στον κώδικα του συμβολαίου, ή ο κώδικας είναι σωστός, αλλά το διαμέρισμά κατασχεθεί πριν φτάσει η ημερομηνία ενοικίασης; Εάν αυτό ήταν ένα παραδοσιακό συμβόλαιο, θα γινόταν απλά να το καταγγείλει κάποιος στο δικαστήριο, αλλά το blockchain αποτελεί μια εντελώς διαφορετική κατάσταση. Το smart contract εκτελεί τον κώδικα που έχει, ανεξάρτητα από το τι μπορεί να προκύψει. Αν αυτές οι περιπτώσεις δεν υπάρχουν στον κώδικα του smart contract, το συμβόλαιο συνεχίζει να λειτουργεί κανονικά. Σε μια τέτοια περίπτωση θα πρέπει να παρατηθεί και να δημιουργηθεί ένα νέο συμβόλαιο.

Οι εμπειρογνώμονες προσπαθούν να τα ξεπεράσουν εξελίσσοντας την τεχνολογία και βρίσκοντας νέους τρόπους, αλλά αυτά τα κρίσιμα ζητήματα αποθαρρύνουν τους πιθανούς υιοθετητές της τεχνολογίας από την χρήση αυτών των συμβολαίων.(Jimmy Song, 2018).

Smart Contracts στο Blockchain

Αυτή τη στιγμή υπάρχουν πολλά blockchains που υποστηρίζουν τα smart contracts, αλλά το μεγαλύτερο είναι το Ethereum.

Μερικά από αυτά είναι:

Bitcoin: Το Bitcoin είναι ιδανικό για την επεξεργασία συναλλαγών Bitcoin, αλλά έχει περιορισμένες δυνατότητες επεξεργασίας εγγράφων.

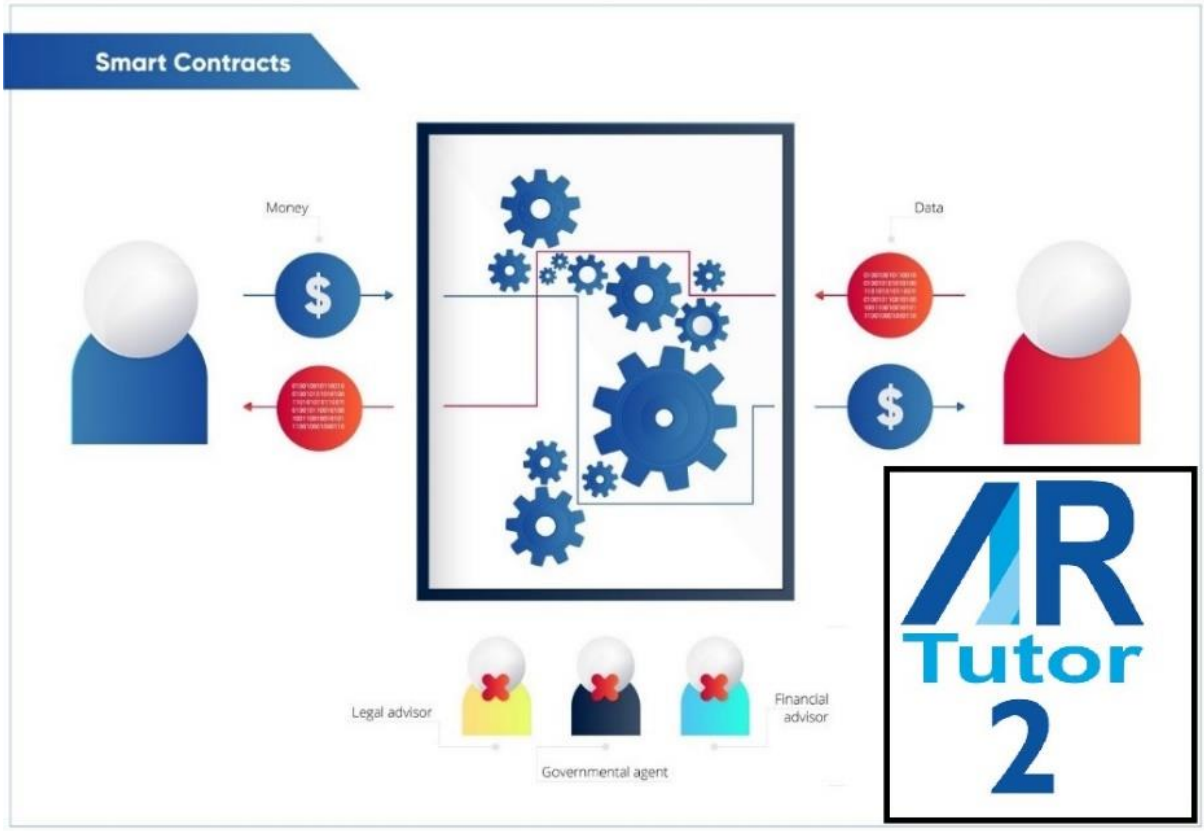
Side Chains: Αυτό είναι ένα άλλο όνομα για τα blockchains που τρέχουν δίπλα στο Bitcoin και προσφέρουν περισσότερα περιθώρια επεξεργασίας συμβολαίων.

NXT: Το NXT είναι μια δημόσια πλατφόρμα blockchain που περιέχει μια περιορισμένη επιλογή προτύπων για smart contracts. Τα οποία περιορίζονται στις δυνατότητες που δίνοται και δεν μπορούν να κωδικοποιηθούν ελεύθερα.

Ethereum: Το Ethereum είναι μια δημόσια πλατφόρμα blockchain και το πιο προηγμένο για την κωδικοποίηση και την επεξεργασία των smart contracts. Σου επιτρέπει να κωδικοποιήσεις ότι επιθυμείς αλλά θα πρέπει να πληρώσεις για υπολογιστική ισχύ με "ETH" tokens.
Αξίζει να σημειωθεί ότι υπάρχουν πάνω από 1 εκατομμύριο smart contracts στο blockchain του Ethereum.

Το Ethereum δημιουργήθηκε και σχεδιάστηκε για να υποστηρίζει τα smart contracts.
Μπορούν να προγραμματιστούν σε μια ειδική γλώσσα προγραμματισμού που ονομάζεται Solidity.
Αυτή η γλώσσα δημιουργήθηκε ειδικά για το Ethereum και χρησιμοποιεί μια σύνταξη που μοιάζει με αυτήν της Javascript.
Αξίζει να σημειωθεί επίσης ότι και το Bitcoin έχει υποστήριξη για smart contracts, αν και είναι πολύ πιο περιορισμένο σε σύγκριση με το Ethereum.

Όσον αφορά τις δυνατότητες των ίδιων των smart contracts, δεν υπάρχει περιορισμός στον κλάδο των βιομηχανιών που μπορεί να επηρεάσει, από την υγειονομική περίθαλψη, τις αυτοκινητοβιομηχανίες έως τις ακίνητες περιουσίες και τη νομοθεσία.(Yessi Bello Perez, 2019). (blockchainhub, 2017).



1 Smart Contract (lisk.io, 2019).

Αναφορές

Hertig, A. (2017). How Do Ethereum Smart Contracts Work? Coindesk. Retrieved from https://www.coindesk.com/information/ethereum-smart-contracts-work/

Rosic, A. (2017). Smart Contracts: The Blockchain Technology That Will Replace Lawyers. Blockgeeks. Retrieved from https://www.coindesk.com/information/ethereum-smart-contracts-work/

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

K, L. (2017). What is Blockchain and Smart Contracts? Brief introduction. Retrieved from https://medium.com/startup-grind/gentle-intro-to-blockchain-and-smart-contracts-part-1-3328afca62ab

Solidity. (2017). Stiftung Ethereum. Retrieved from http://solidity.readthedocs.io/en/latest/

Smart contract. (2019, March 02). Retrieved from https://en.wikipedia.org/wiki/Smart_contract

Buterin, Vitalik. "Ethereum Whitepaper". github. Retrieved May 12, 2019.

Atzei, Nicola; Bartoletti, Massimo; Cimoli, Tiziana (2017), "A survey of attacks on Ethereum smart contracts" (PDF), 6th International Conference on Principles of Security and Trust (POST), European Joint Conferences on Theory and Practice of Software

Nick Szabo (2005). "Secure Property Titles with Owner Authority". Archived from the original on January 15, 2014. Retrieved May 12, 2019.

Ross, Rory (2015-09-12). "Smart Money: Blockchains Are the Future of the Internet". Newsweek. Retrieved May 12, 2019.

Lewis, A., & Lewis, A. (2018, August 04). A gentle introduction to Ethereum – Bits on Blocks. Retrieved from https://bitsonblocks.net/2016/10/02/gentle-introduction-ethereum/

S., J. (2018, May 06). How does blockchain work in 7 steps - A clear and simple explanation. Retrieved from https://blog.goodaudience.com/blockchain-for-beginners-what-is-blockchain-519db8c6677a

Lewis, A., & Lewis, A. (2018, October 30). A Gentle Introduction to Blockchain Technology – Bits on Blocks. Retrieved from https://bitsonblocks.net/2015/09/09/gentle-introduction-blockchain-technology/

What is Ethereum? [The Most Comprehensive Beginners Guide]. (n.d.). Retrieved from https://blockgeeks.com/guides/ethereum/